PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-226390

(43)Date of publication of application : 25.08.2005

(51)Int.Cl. E05B 49/00
B60R 25/00
B60R 25/10
H04B 1/38
H04Q 7/38

(21)Application number : 2004-038023

(22)Date of filing : 16.02.2004

(71)Applicant : TOKAI RIKA CO LTD
TOYOTA MOTOR CORP

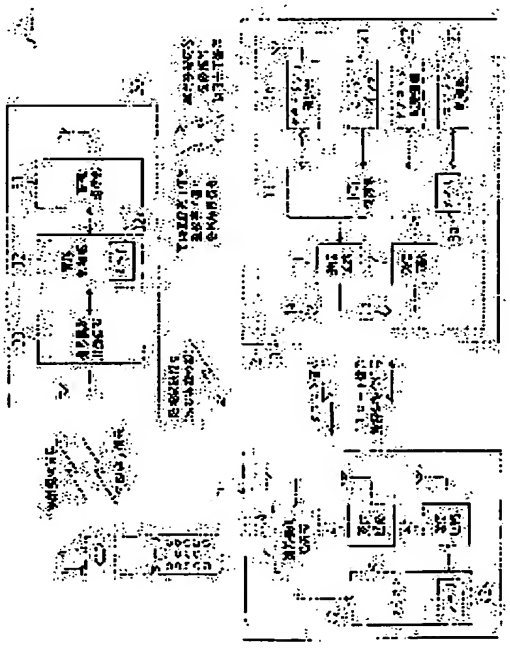
(72)Inventor : KAWAMURA DAISUKE
KIMURA AKITO
YAMAMOTO KEIJI
SHOMURA KOICHI
OZAWA TAKAO
NAKANE YOSHIFUSA

(54) SECURITY CONTROL SYSTEM, SECURITY CONTROLLER, CONTROLLER IN SECURITY CONTROL SYSTEM AND METHOD FOR CONTROLLING SECURITY

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a security control system capable of further improving the security level of security equipment, a security controller, a controller in the security control system and a method for controlling a security.

SOLUTION: The security controller 10 collates an ID code set to a portable machine 3 and the ID code previously recorded to a memory 13a by a communication with the portable machine 3, and controls a door-lock driving device 22 and an engine control section 23 on the basis of the presence of the organization of the collation. The controller 30 transmits a function limiting signal to the security controller 10 under the condition of the input of a limit requirement signal from a portable telephone 4. The security controller 10 inhibits or limits the control of the security equipment (the door-lock driving device 22 and the engine control section 23) based on the communication with the portable machine 3 when the



security controller 10 receives the function limiting signal.

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]
While performing collation with portable apparatus which has a communication function, and an ID code set as this portable apparatus and an ID code already recorded on an own recording device based on communication with this portable apparatus, By controlling security equipments based on the collated result, it is the security control system provided with a security control device which controls security releasing operation by these security equipments, and a controlling device which performs communication with this security control device,
Said controlling device transmits a function restriction signal to either [at least] said portable apparatus or said security control device, on condition that a restriction requirement signal was inputted,
A security control system, wherein said security control device forbids or restricts control of said security equipments based on communication with said portable apparatus at the time of receiving said function restriction signal, or communication with said portable apparatus which received said function restriction signal.
[Claim 2]
The security control system according to claim 1 when said security control device receives said function restriction signal, wherein it forbids the communication with said portable apparatus itself.
[Claim 3]
When said portable apparatus receives said function restriction signal, it transmits a sending signal containing a function restriction code at the time of communication with said security control device,
The security control system according to claim 1 or 2 forbidding or restricting control of said security equipments on condition that said security control device received said sending signal.
[Claim 4]

Said restriction requirement signal is transmitted from a portable transmitter machine possessed by user apart from said portable apparatus,
A security control system given in any 1 paragraph of claims 1-3 on condition that it had a reception means which receives said restriction requirement signal and said controlling device was inputted [said restriction requirement signal] via this reception means, wherein it transmits said function restriction signal.
[Claim 5]
While said security control device performs ID registration control which records an ID code set as said portable apparatus on said recording device based on communication with this portable apparatus, At the time of communication with said portable apparatus at the time of receiving said function restriction signal, or communication with said portable apparatus which received said function restriction signal. A security control system given in any 1 paragraph of claims 1-4 forbidding control of said security equipments based on communication with this portable apparatus by forbidding this ID registration control.
[Claim 6]
A means of communication for portable apparatus which performs communication with portable apparatus with which a peculiar ID code was set up,
A recording device on which said ID code and a corresponding ID code are recorded,
A security control means to control security equipments based on whether performed collation with an ID code set as portable apparatus, and an ID code recorded on said recording device at the time of communication with said portable apparatus, and this collation was in agreement,
It has a controlling device and a security communication means which can be communicated which are allocated in the exterior of the security control device concerned,
A security control device forbidding or restricting security releasing operation by said security equipments on condition that said security control means received a function restriction signal transmitted from said controlling device by said security communication means.
[Claim 7]
The security control device according to claim 6 when said security control means receives said function restriction signal by said security communication means, wherein it forbids the communication with said portable apparatus itself.
[Claim 8]
While said security control means performs ID registration control which records an ID code set as said portable apparatus on said recording device based on communication with this portable apparatus, The security control device according to claim 6 or 7 forbidding or restricting control of said security equipments based on communication with this portable apparatus by forbidding this ID registration control when said security communication means receives said function restriction signal.
[Claim 9]

A management means of communication which controls security equipments based on a collated result of an ID code set as this portable apparatus, and an ID code beforehand registered into self based on communication with portable apparatus which has a communication function and in which a security control device and communication are possible, And at least one of said portable apparatus and the means of communication for portable apparatus which can be communicated,
A function restriction signal for making security releasing operation by said security equipments forbid or restrict, on condition that a restriction requirement signal was inputted via said management means of communication or said means of communication for portable apparatus, A controlling device in a security control system provided with a restriction control means which transmits to either [at least] said security control device or said portable apparatus.
[Claim 10]
It has a means of communication for portable devices which performs communication with a portable transmitter machine possessed by user,
A controlling device in the security control system according to claim 9, wherein this means of communication for portable devices receives a restriction requirement signal transmitted from said portable transmitter machine and inputs the restriction requirement signal into said restriction control means.
[Claim 11]
While communication with portable apparatus which has a communication function performs collation with an ID code set as portable apparatus, and an ID code already recorded on an own recording device, A security control device which controls security releasing operation by these security equipments by controlling security equipments based on the collated result, It is the security control method in a security control system provided with a controlling device which performs communication with this security control device,
When a restriction requirement signal of a purport that function restriction is performed from a user to said controlling device is inputted, a function restriction signal is transmitted from this controlling device to either [at least] said portable apparatus or said security control device,
A security control method characterized by making security releasing operation by said security equipments forbid or restrict at the time of communication with said portable apparatus at the time of said security control device receiving said function restriction signal, or communication with said portable apparatus which received said function restriction signal.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[Field of the Invention]
[0001]
This invention relates to the security control system and security control device which are used for vehicles, a residence, etc., for example, the controlling device in this security control system, and the security control method.
[Background of the Invention]
[0002]
Generally, it is operational in security equipments, such as vehicles and a door lock device of a residence, using the machine key for exclusive use possessed by the user. However, since there is a possibility that security equipments may be unjustly operated by copying a machine key unjustly in this case, or performing picking etc., it is regarded as questionable socially.
[0003]
Then, in order to aim at improvement in the security level of security equipments conventionally, the security control system which used electronic collation, for example is proposed (for example, refer to the patent documents 1 and patent documents 2).
[0004]
As shown in these patent documents 1 and 2, in the security control system for vehicles, radio is performed between the portable apparatus possessed by the user and the security control device allocated by vehicles. If the ID code signal which specifically contains the peculiar ID code set as portable apparatus is transmitted to a security control device from portable apparatus, a security control device will perform comparison with the ID code contained in this ID code signal, and the ID code beforehand registered into self. And when these ID codes of a security control device correspond, it judges that communication with portable apparatus was materialized, makes a door lock unlock or performs engine start-up permission. That is, a security control device performs security releasing operation of various security equipments, on condition that communication with portable apparatus was

materialized. For this reason, the security releasing operation by the third party who does not possess corresponding portable apparatus becomes impossible, and a security level improves.

[Patent documents 1] JP,2001-289142,A

[Patent documents 2] JP,2001-311333,A

[Description of the Invention]

[Problem(s) to be Solved by the Invention]

[0005]

However, in the conventional security control device for vehicles, when the user of what can acquire the theft preventive effect outstanding in the anticipated-use state loses portable apparatus or the theft of this portable apparatus is carried out, there is a possibility that this portable apparatus may be used by the third party. Thus, in the conventional security control system for vehicles, although it is a special case, a thoroughgoing theft preventive effect may not be acquired.

[0006]

So, in the former, it is requested that the security level of security equipments is made still higher.

This invention is made in view of such the actual condition, and the purpose, It is in providing the security control system and security control device which can raise the security level of security equipments further, the controlling device in a security control system, and the security control method.

[Means for Solving the Problem]

[0007]

In order to solve the above-mentioned technical problem, in the invention according to claim 1. While performing collation with portable apparatus which has a communication function, and an ID code set as this portable apparatus and an ID code already recorded on an own recording device based on communication with this portable apparatus, A security control device which controls security releasing operation by these security equipments by controlling security equipments based on the collated result, Are a controlling device which performs communication with this security control device the security control system which it had, and said controlling device, On condition that a restriction requirement signal was inputted, transmit to either [at least] said portable apparatus or said security control device, and a function restriction signal said security control device, Let it be a gist to forbid or restrict control of said security equipments based on communication with said portable apparatus at the time of receiving said function restriction signal, or communication with said portable apparatus which received said function restriction signal.

[0008]

In the invention according to claim 2, in the security control system according to claim 1, when said security control device receives said function restriction signal, it makes it a gist to forbid the communication with said portable apparatus itself.

[0009]
In the invention according to claim 3, in the security control system according to claim 1 or 2, said portable apparatus, When said function restriction signal is received, at the time of communication with said security control device, a sending signal containing a function restriction code is transmitted, and said security control device makes it a gist to forbid or restrict control of said security equipments, on condition that said sending signal was received.
[0010]
In the invention according to claim 4, in any 1 paragraph of claims 1-3, in a security control system of a statement said restriction requirement signal, It is transmitted from a portable transmitter machine possessed by user apart from said portable apparatus, and said controlling device is provided with a reception means which receives said restriction requirement signal, and let it be a gist to transmit said function restriction signal, on condition that said restriction requirement signal was inputted via this reception means.
[0011]
In the invention according to claim 5, in any 1 paragraph of claims 1-4, in a security control system of a statement said security control device, While performing ID registration control which records an ID code set as said portable apparatus on said recording device based on communication with this portable apparatus, Let it be a gist to forbid control of said security equipments based on communication with this portable apparatus by forbidding this ID registration control at the time of communication with said portable apparatus at the time of receiving said function restriction signal, or communication with said portable apparatus which received said function restriction signal.
[0012]
A means of communication for portable apparatus which performs communication with portable apparatus with which a peculiar ID code was set up in the invention according to claim 6, At the time of communication with a recording device on which said ID code and a corresponding ID code are recorded, and said portable apparatus. A security control means to control security equipments based on whether performed collation with an ID code set as portable apparatus, and an ID code recorded on said recording device, and this collation was in agreement, Have a controlling device and a security communication means which can be communicated which are allocated in the exterior of the security control device concerned, and said security control means, Let it be a gist to forbid or restrict security releasing operation by said security equipments, on condition that a function restriction signal transmitted from said controlling device was received by said security communication means.
[0013]
In the invention according to claim 7, in the security control device according to claim 6, when said security control means receives said function restriction signal by said security communication means, it makes it a gist to forbid the communication with said portable

apparatus itself.

[0014]

In the invention according to claim 8, in the security control device according to claim 6 or 7, said security control means, While performing ID registration control which records an ID code set as said portable apparatus on said recording device based on communication with this portable apparatus, When said security communication means receives said function restriction signal, let it be a gist to forbid or restrict control of said security equipments based on communication with this portable apparatus by forbidding this ID registration control.

[0015]

In the invention according to claim 9, based on communication with portable apparatus which has a communication function, A management means of communication which controls security equipments based on a collated result of an ID code set as this portable apparatus, and an ID code beforehand registered into self and in which a security control device and communication are possible, And at least one of said portable apparatus and the means of communication for portable apparatus which can be communicated, A function restriction signal for making security releasing operation by said security equipments forbid or restrict, on condition that a restriction requirement signal was inputted via said management means of communication or said means of communication for portable apparatus, Let it be a gist to have a restriction control means which transmits to either [at least] said security control device or said portable apparatus.

[0016]

In a controlling device [in / by the invention according to claim 10 / the security control system according to claim 9], Having a means of communication for portable devices which performs communication with a portable transmitter machine possessed by user, this means of communication for portable devices receives a restriction requirement signal transmitted from said portable transmitter machine, and makes it a gist to input the restriction requirement signal into said restriction control means.

[0017]

In the invention according to claim 11, by communication with portable apparatus which has a communication function, while performing collation with an ID code set as portable apparatus, and an ID code already recorded on an own recording device, A security control device which controls security releasing operation by these security equipments by controlling security equipments based on the collated result, It is the security control method in a security control system provided with a controlling device which performs communication with this security control device, When a restriction requirement signal of a purport that function restriction is performed from a user to said controlling device is inputted, A function restriction signal is transmitted from this controlling device to either [at least] said portable apparatus or said security control device, Let it be a gist to make security releasing operation by said security equipments forbid or restrict at the time of

communication with said portable apparatus at the time of said security control device receiving said function restriction signal, or communication with said portable apparatus which received said function restriction signal.

[0018]

Hereafter, "OPERATION" of this invention is explained.

If a restriction requirement signal is received by controlling device according to the invention given in claims 1 and 11, a function restriction signal will be transmitted from this controlling device to either [at least] portable apparatus or the security control devices. And a security control device forbids or restricts control of security equipments based on communication with portable apparatus at the time of receiving this function restriction signal, and communication with portable apparatus which received this function restriction signal. For this reason, when a user loses portable apparatus or a theft is carried out, security releasing operation by a security control device can be forbidden or restricted by taking a measure of inputting a restriction requirement signal into a controlling device. Therefore, at the time of loss and a theft of portable apparatus, security releasing operation which used this portable apparatus can be forbidden or restricted, and a high security level of security equipments can be secured.

[0019]

According to the invention according to claim 2, a security control device will forbid the communication with portable apparatus itself, if a function restriction signal from a controlling device is received. That is, a security control device will forbid security releasing operation based on communication with portable apparatus, if a function restriction signal is received. For this reason, at the time of loss and a theft of portable apparatus, security releasing operation which used this portable apparatus is forbidden certainly. Therefore, it becomes possible to secure a high security level of security equipments.

[0020]

According to the invention according to claim 3, portable apparatus will transmit a sending signal containing a function restriction code at the time of communication with a security control device, if a function restriction signal is received. On the other hand, a security control device forbids or restricts security control operation, on condition that a sending signal containing this function restriction code was received. For this reason, at the time of loss and a theft of portable apparatus, security releasing operation which used this portable apparatus is forbidden or restricted certainly. Therefore, it becomes possible to secure a high security level of security equipments.

[0021]

If a restriction requirement signal which is transmitted from a portable transmitter machine which a user possesses according to the invention according to claim 4 is received by controlling device, a function restriction signal will be transmitted from a controlling device to a security control device. For this reason, when a user loses portable apparatus or a theft is carried out, security releasing operation can be forbidden or restricted by making a

restriction requirement signal transmit from a portable transmitter machine. Therefore, at the time of loss and a theft of portable apparatus, security releasing operation by this portable apparatus can be forbidden or restricted immediately, and it becomes possible to secure a high security level of security equipments.

[0022]

According to the invention according to claim 5, a security control device forbids ID registration control at the time of communication with portable apparatus at the time of receiving a function restriction signal, or communication with portable apparatus which received a function restriction signal. For this reason, communication with this portable apparatus and a security control device stops materializing, and security releasing operation using this portable apparatus is forbidden certainly. Therefore, unjust registration of an ID code by a third party can be prevented, and it becomes possible to secure a high security level of security equipments.

[0023]

If a function restriction signal which is transmitted from a controlling device according to the invention according to claim 6 is received by security communication means, a security control means will forbid or restrict security releasing operation by security equipments. For this reason, if it is made to make a restriction requirement signal transmit from a controlling device by a measure by a user when a user loses portable apparatus, for example or a theft is carried out, security releasing operation by a security control device can be forbidden or restricted. Therefore, at the time of loss and a theft of portable apparatus, security releasing operation which used this portable apparatus can be forbidden or restricted, and a high security level of security equipments can be secured.

[0024]

If a security communication means receives a function restriction signal from a controlling device according to the invention according to claim 7, a security control means will forbid the communication with portable apparatus itself, and will forbid security releasing operation based on communication with portable apparatus. For this reason, if it is made to make a restriction requirement signal transmit from a controlling device at the time of loss and a theft of portable apparatus for example, security releasing operation using this portable apparatus will be forbidden certainly. Therefore, it becomes possible to secure a high security level of security equipments.

[0025]

According to the invention according to claim 8, a security control means will forbid ID registration control, if a security communication means receives a function restriction signal from a controlling device. Since an ID code set as portable apparatus will not be made into a recording device, communication with portable apparatus and a security control device stops that is, materializing. For this reason, communication with this portable apparatus and a security control device stops materializing, and security releasing operation using this portable apparatus is forbidden certainly. Therefore, unjust registration of an ID code by a

third party can be prevented, and it becomes possible to secure a high security level of security equipments.

[0026]

When a controlling device is provided with a management means of communication according to the invention according to claim 9, a restriction control means will transmit a function restriction signal to a security control device via this management means of communication, if a restriction requirement signal is inputted. For this reason, this function restriction signal will be inputted into a security control device. When a controlling device is provided with a means of communication for portable apparatus, a restriction control means will transmit a function restriction signal to portable apparatus via this means of communication for portable apparatus, if a restriction requirement signal is inputted. For this reason, this function restriction signal will be inputted into portable apparatus. Therefore, for example, if it is made to make a function restriction signal transmit to a security control device from portable apparatus at the time of communication with portable apparatus and a security control device, this function restriction signal will be inputted into a security control device. Since a function restriction signal is a signal for making security releasing operation by security equipments forbid or restrict, a security control device will forbid or restrict security releasing operation, if this function restriction signal is inputted. Therefore, in the case of which [of these], at the time of loss and a theft of portable apparatus, security releasing operation using this portable apparatus can be forbidden or restricted in a user inputting a restriction requirement signal into a controlling device. So, a high security level of security equipments is securable.

[0027]

According to the invention according to claim 10, it is transmitted from a portable transmitter machine possessed by user, and a restriction requirement signal is received by means of communication for portable devices. Thereby, this restriction requirement signal is inputted into a restriction control means. For this reason, when a user loses portable apparatus or a theft is carried out, security releasing operation can be forbidden or restricted by making a restriction requirement signal transmit from a portable transmitter machine. Therefore, at the time of loss and a theft of portable apparatus, security releasing operation by this portable apparatus can be forbidden or restricted immediately, and it becomes possible to secure a high security level of security equipments.

[Effect of the Invention]

[0028]

As explained in full detail above, according to this invention, the security level of security equipments can be raised further.

[Best Mode of Carrying Out the Invention]

[0029]

Hereafter, one embodiment which materialized this invention to the security control system for vehicles is described in detail based on drawing 1 - drawing 4.

As shown in drawing 1, the security control system 1 for vehicles is provided with the following.
Portable apparatus 3 possessed by the user (owner) of the vehicles 2.
The security control device 10 formed in the vehicles 2.
The controlling device 30 formed in the prescribed spot of the vehicles exterior.

[0030]
The receiving circuit 41 which receives the request signal which the portable apparatus 3 has a communication function and is transmitted from the security control device 10, It has the microcomputer (microcomputer) 42 into which the received request signal is inputted, and the sending circuit 43 which transmits the ID code signal and lock/unlock command signal which are outputted from the microcomputer 42.
[0031]
The receiving circuit 41 restores to the received request signal to a pulse signal, and outputs it to the microcomputer 42. The sending circuit 43 modulates the ID code signal and lock/unlock command signal which are outputted from the microcomputer 42 on the electric wave of predetermined frequency, and transmits outside.
[0032]
The microcomputer 42 is a CPU unit which consists of CPU, ROM, RAM, etc. which are not illustrated, and is specifically provided with the nonvolatile memory 42a. The ID code individually set up for every portable apparatus is beforehand recorded on this memory 42a.
[0033]
And if a request signal is inputted from the receiving circuit 41, the microcomputer 42 will read an ID code from the memory 42a, and will transmit the ID code signal containing this ID code to the sending circuit 43. The final controlling element which was provided in the design surface of the portable apparatus 3 and which is not illustrated is electrically connected to the microcomputer 42. And if this final controlling element is operated, a manipulate signal will be inputted into the microcomputer 42, and this microcomputer 42 outputs the lock/unlock command signal containing an ID code, and a locking code or a unlocking code to the sending circuit 43.
[0034]
The security control device 10 is provided with the following.
The sending circuit 11 and the receiving circuit 12 as a means of communication for portable apparatus.
The vehicle control part 13 as a security control means.
The security communication part 14 as a security communication means.
And the sending circuit 11, the receiving circuit 12, and the security communication part 14 are electrically connected to the vehicle control part 13.
[0035]

The sending circuit 11 changes into the electric wave of predetermined frequency (here 134 kHz) the request signal outputted from the vehicle control part 13, and transmits this electric wave to the surrounding predetermined region of the vehicles 2, and the interior of a room of the vehicles 2 selectively via the transmission antenna 11a.

[0036]

The receiving circuit 12 receives the ID code signal and lock/unlock command signal which are transmitted from the portable apparatus 3 via the receiving antenna 12a, restores to the input signal to a pulse signal, and outputs it to the vehicle control part 13.

[0037]

The security communication part 14 is constituted so that the controlling device 30 and communication are possible. And if a registered signal is inputted from the vehicle control part 13, the security communication part 14 will modulate the registered signal on the electric wave of predetermined frequency, and will transmit this electric wave to the controlling device 30. It will restore to this sending signal to a pulse signal, and the security communication part 14 will output the signal to which it this restored to the vehicle control part 13, if the sending signal transmitted from the controlling device 30 is received.

[0038]

The vehicle control part 13 is a CPU unit which consists of CPU, ROM, and RAM which are not illustrated, and is specifically provided with the nonvolatile memory 13a as a recording device. In this memory 13a, one or more records of the ID code set as the portable apparatus 3 are possible.

[0039]

The mode switch 21, and the door lock drive device 22 and Engine control section 23 as security equipments are electrically connected to the vehicle control part 13.

The mode switch 21 is an operational switch and is provided in the interior of a room of the vehicles 2 by the user in this embodiment. And operation of this mode switch 21 will output a manipulate signal to these mode switch 21 empty-vehicle both control sections 13.

[0040]

If it is connected to the actuator which is not illustrated and a driving signal is inputted from the vehicle control part 13, the door lock drive device 22 will drive this actuator, and will carry out lock/unlock of the door lock automatically. The door lock drive device 22 outputs the lock/unlock condition signal which shows the lock/unlock state of a door lock to the vehicle control part 13. For this reason, based on this lock/unlock condition signal, recognition of the lock/unlock state of a door lock of the vehicle control part 13 is attained.

[0041]

It performs fuel injection control and ignition control, and starts an engine automatically while driving the starter, if it is connected to the starter which is not illustrated and Engine control section 23 is inputted [a start signal] from the vehicle control part 13. Engine control section 23 outputs the driving state signal which shows an engine driving state to the vehicle control part 13. For this reason, based on this driving state signal, recognition of

an engine driving state of the vehicle control part 13 is attained.

[0042]

The vehicle control part 13 is provided with the following.

Car registration mode.

ID registration mode.

Security control mode.

Here, car registration mode shows the mode in which car registration control which registers the vehicles 2 as an administration object of the controlling device 30 is performed. ID registration mode shows the mode in which ID registration control which records the ID code set as the portable apparatus 3 on the memory 13a (registration) is performed. Security control mode shows the mode which controls the door lock drive device 22 and Engine control section 23 based on communication with the portable apparatus 3 by which ID registration was carried out. And the vehicle control part 13 serves as ID registration mode or car registration mode, when a manipulate signal is inputted from the mode switch 21, and it serves as security control mode except it. That is, the vehicle control part 13 serves as security control mode, and usually switches to ID registration mode or car registration mode by operating the mode switch 21. Although it switches to ID registration mode or car registration mode by operation of the mode switch 21 here, It switches to ID registration mode by operation of not only this but the mode switch 21, and switches to car registration mode by operation of other switches. That is, it switches to ID registration mode or car registration mode by individual operation.

[0043]

If such a vehicle control part 13 switches to car registration mode, it will perform car registration control.

In detail, the input signal from the input device (for example, input parts, such as a car-navigation system) which is not illustrated can be inputted into the vehicle control part 13. And if the password for function restrictions which can be set up by a user is inputted into this input device and the input signal which consists of this password for function restrictions is inputted into the vehicle control part 13 after switching to car registration mode, The vehicle control part 13 transmits the car registration signal containing vehicle information and the password cord for function restrictions to the controlling device 30 via the security communication part 14. Vehicle information is information for specifying the vehicles 2, and at least one of the car body number of the vehicles 2, a fleet number, and dealer information, including a store number, a password, etc. which were set up peculiar to a dealer, is contained in vehicle information in this embodiment. With the password cord for function restrictions, it is equivalent to what carried out binary conversion of the password for function restrictions.

[0044]

If the car registration completion signal transmitted from the controlling device 30 is inputted into the vehicle control part 13 via the security communication part 14, this vehicle control

part 13 will perform the display which shows that registration of the vehicles 2 was completed to the indicator which was formed in the interior of a room of the vehicles 2, and which is not illustrated.

[0045]

On the other hand, if it switches to ID registration mode, the vehicle control part 13 will perform registration communications control.

In detail, the vehicle control part 13 outputs a request signal intermittently to the sending circuit 11, and transmits a request signal to the interior of a room of the vehicles 2 via the sending circuit 11 and the transmission antenna 11a. And if the receiving circuit 12 and the receiving antenna 12a receive the ID code signal from the portable apparatus 3 answered and transmitted to this request signal and an ID code signal is inputted from this receiving circuit 12, The vehicle control part 13 records the ID code contained in this ID code signal on the memory 13a. And if record of this ID code is completed, the vehicle control part 13 will output the registered signal which includes this ID code and vehicle information to the security communication part 14, and will transmit a registered signal to the controlling device 30 via this security communication part 14.

[0046]

On the other hand, in security control mode, the vehicle control part 13 outputs a request signal intermittently to the sending circuit 11. For this reason, a request signal is selectively transmitted to the surrounding predetermined region of the vehicles 2, and the interior of a room of the vehicles 2 via the sending circuit 11 and the transmission antenna 11a. The vehicle control part 13 will perform comparison (ID code collation) with the ID code contained in those signals, and the ID code currently recorded on the memory 13a, if said ID code signal or a lock/unlock command signal is inputted from the receiving circuit 12. And the vehicle control part 13 performs drive controlling of the door lock drive device 22 or Engine control section 23, on condition that these ID codes were in agreement, i.e., ID code collation was materialized.

[0047]

When an ID code signal is inputted, the vehicle control part 13 outputs a driving signal to the door lock drive device 22, and makes a door lock unlock in detail, if this ID code signal answers the request signal transmitted to the surrounding predetermined region of the vehicles 2. And if this ID code signal is no longer inputted, the vehicle control part 13 outputs a driving signal to the door lock drive device 22, and makes a door lock lock.

[0048]

On the other hand, the vehicle control part 13 will be in an engine start waiting state, if the inputted ID code signal answers the request signal transmitted to the interior of a room of the vehicles 2. And if a manipulate signal is inputted from the start switch which is not illustrated in this engine start waiting state, the vehicle control part 13 will output a start signal to Engine control section 23, and will start an engine. That is, when it is not an engine start waiting state, the vehicle control part 13 will not output a start signal to Engine

control section 23, even if a manipulate signal is inputted from a start switch. A start switch is a switch formed near the driver's seat in the interior of a room of the vehicles 2, and is electrically connected with the vehicle control part 13.

[0049]

The vehicle control part 13 will make a door lock lock, if the locking code is contained in this lock/unlock command signal, and if the unlocking code is contained, it will make a door lock unlock, when a lock/unlock command signal is inputted.

[0050]

Thus, in security control mode, the security control device 10 performs communication with the portable apparatus 3, and controls security equipments, such as the door lock drive device 22 and Engine control section 23, based on the formation existence of communication with this portable apparatus 3.

[0051]

The controlling device 30 is allocated in the control center for exclusive use etc., and is provided with the management communications department 31 as a management means of communication, the supervisory control part 32 as a restriction control means, and the communications department 33 for portable devices as the means of communication for portable devices, and a reception means. And the management communications department 31 and the communications department 33 for portable devices are electrically connected to the supervisory control part 32.

[0052]

The security communication part 14 of the security control device 10 and communication of the management communications department 31 are attained, and if the car registration signal and registered signal which are transmitted from this security communication part 14 are received, it will restore to these signals and will output to the supervisory control part 32.

[0053]

The portable transmitter machine (here cellular phone 4) possessed by the user and communication are possible for the communications department 33 for portable devices. The cellular phone 4 judges that restriction operation was performed, when said password for function restrictions is inputted from a ten key, and it transmits the restriction requirement signal containing the password cord for function restrictions which carried out binary conversion of this password for function restrictions to the controlling device 30. the password for function restrictions -- when the portable apparatus designation number which specifies both the portable apparatus 3 is inputted from a ten key, the cellular phone 4 transmits the restriction requirement signal containing the password cord for function restrictions, and a portable apparatus designation code to the controlling device 30. Here, a portable apparatus designation number shows the registration number of the ID code recorded on the memory 32a of said controlling device 30, and it is equivalent to what carried out binary conversion of this portable apparatus designation number with a portable

apparatus designation code.

[0054]

And if the restriction requirement signal transmitted from the cellular phone 4 is received, the communications department 33 for portable devices will restore to this restriction requirement signal, and will output to the supervisory control part 32. The communications department 33 for portable devices will transmit the restriction completion signal to the cellular phone 4 using a public network etc., if a restriction completion signal is inputted from the supervisory control part 32. The cellular phone 4 will notify a user of that by a sound, vibration, display, etc., if the restriction completion signal transmitted from the communications department 33 for portable devices is received.

[0055]

The supervisory control part 32 is a CPU unit which consists of CPU, ROM, and RAM which are not illustrated, and is specifically provided with the nonvolatile memory 32a. The vehicle information of the vehicles 2 set up as an administration object is recorded on this memory 32a. In detail, the information for specifying the vehicles 2, including the car body number of the vehicles 2, a fleet number, dealer information, the equipment information (a telephone number, a mail address, etc.) of said cellular phones (a store number, a password, etc. which were set up peculiar to a dealer) 4, etc., is recorded on the memory 32a as vehicle information.

[0056]

The password cord for function restrictions transmitted from the security control device 10 at the time of said car registration control and the ID code transmitted from the security control device 10 at the time of said registration communications control can record on the memory 32a in the state where it was matched with vehicle information, respectively. In detail, corresponding to this vehicle information, the record section of the password cord for function restrictions and the record section (ID record section) of the ID code are set to the memory 32a. For example, when the vehicle information A and B of the two vehicles 2 is recorded on the memory 32a, the record section of the password cord for function restrictions corresponding to the vehicle information A and ID record section, and the record section and ID record section of the password cord for function restrictions corresponding to the vehicle information B are set up individually. It is this ID record section recordable about two or more ID codes, and the number of the ID codes in which the record is possible is the prescribed number set up by the prescribed number set up beforehand or the user. The registration number which consists of turn etc. which were recorded, for example is matched with the ID code recorded on this record section.

[0057]

The supervisory control part 32 will record the vehicle information and the password cord for function restrictions which are contained in this car registration signal on the memory 32a in the state where it matched, if management communications department 31 empty-vehicle both registered signals are inputted. And the supervisory control part 32 transmits

the car registration completion signal which shows that car registration was completed to the security control device 10 via the management communications department 31.

[0058]

The supervisory control part 32 will record the ID code contained in the registered signal on the vehicle information included in this registered signal, and corresponding ID record section, if a registered signal is inputted from the management communications department 31. And the supervisory control part 32 transmits the registration completion signal which shows that this record was completed to the security control device 10 via the management communications department 31.

[0059]

If a restriction requirement signal is inputted from the communications department 33 for portable devices, the supervisory control part 32, From the password cord for function restrictions already recorded on the memory 32a, the existence of the password cord for function restrictions contained in this restriction requirement signal and the corresponding password cord for function restrictions is judged (password cord existence judgment). As a result, when the password cord for function restrictions contained in a restriction requirement signal and the corresponding password cord for function restrictions exist in the memory 32a, the supervisory control part 32 specifies the vehicles 2 used as the administration object of restriction instruction control based on this password cord for function restrictions, and corresponding vehicle information. And the supervisory control part 32 transmits the function restriction signal containing a function restriction code via the management communications department 31 to the security control device 10 carried in the specified vehicles 2. When said portable apparatus designation code is contained in the restriction requirement signal, the supervisory control part 32 reads the ID code with which the registration number which is in agreement with a portable apparatus designation code among the ID codes recorded on the memory 32a corresponding to vehicle information was matched. And the supervisory control part 32 transmits the function restriction signal containing the read ID code and said function restriction code via the management communications department 31. The supervisory control part 32 will transmit this restriction completion signal to the cellular phone 4 via the communications department 33 for portable devices, if a restriction completion signal is inputted from the management communications department 31.

[0060]

On the other hand, the security control device 10 will perform function restriction processing which restricts or forbids the drive of the door lock drive device 22 or Engine control section 23 based on communication with the portable apparatus 3 mentioned above, if the function restriction signal transmitted from the controlling device 30 is received.

[0061]

In detail, the security control device 10 receives a function restriction signal by the security communication part 14 first. For this reason, this function restriction signal is inputted into

the vehicle control part 13. The vehicle control part 13 will transmit the restriction completion signal which shows that it changed into the state of performing function restriction processing to the controlling device 30 via the security communication part 14, if a function restriction signal is inputted. The vehicle control part 13 judges whether the ID code is contained in this function restriction signal. As a result, when the ID code is not contained in the function restriction signal, the vehicle control part 13 restricts or forbids control of the door lock drive device 22 or Engine control section 23, even if communication with which portable apparatus 3 which can communicate is materialized. That is, even if communication with the portable apparatus 3 with which the vehicle control part 13 corresponds in this case with all the ID codes currently recorded on the memory 13a is materialized, security release of security equipments (the door lock drive device 22 and Engine control section 23) is restricted or forbidden. Only when communication with the portable apparatus 3 with which the vehicle control part 13 corresponds with this ID code when the ID code is contained in the function restriction signal is materialized, control of the door lock drive device 22 or Engine control section 23 is restricted or forbidden.

[0062]

In this embodiment, the vehicle control part 13 can be set up by a user about which processing of these function restriction processing shown in the following <a> or <b> is performed, and is performed.

[0063]

The <a> 1st function restriction processing (security release prohibition process)

(a-1) When the ID code is not contained in the function restriction signal

In this case, if the ID code signal from the portable apparatus 3 and the lock/unlock command signal from the portable apparatus 3 which were answered and transmitted to the request signal are received, the vehicle control part 13, Though the ID code contained in these ID code signals or a lock/unlock command signal was recorded on the memory 13a, control of the door lock drive device 22 or Engine control section 23 is not performed. That is, the vehicle control part 13 forbids unlocking of a door lock, and engine start up, even if communication with the portable apparatus 3 is materialized. If it puts in another way, and a function restriction signal is inputted, the vehicle control part 13 will forbid security releasing operation called start-up permission of the engine by unlocking and Engine control section 23 of the door lock by the door lock drive device 22.

[0064]

(a-2) When the ID code is contained in the function restriction signal

In this case, the vehicle control part 13 compares first the ID code contained in this ID code signal or a lock/unlock command signal with the ID code contained in a function restriction signal, if the ID code signal from the portable apparatus 3 and the lock/unlock command signal from the portable apparatus 3 which were answered and transmitted to the request signal are received. As a result, the vehicle control part 13 is restricted when these ID codes are in agreement, and it does not perform control of the door lock drive device 22 or

Engine control section 23. That is, only when communication with the portable apparatus 3 with which the vehicle control part 13 corresponds with the ID code contained in a function restriction signal in this case is materialized, unlocking of a door lock and engine start up, i.e., security releasing operation, are forbidden. Therefore, the vehicle control part 13 performs security releasing operation as usual, when the ID code signal and lock/unlock command signal containing other ID codes (ID code which is not contained in the functional limiting signal) recorded on the memory 13a are received. That is, only the security releasing operation using the specific portable apparatus 3 is forbidden here.

[0065]

The <b> 2nd function restriction processing (security release restriction processing)

(b-1) When the ID code is not contained in the function restriction signal

In this case, if the ID code signal from the portable apparatus 3 and the lock/unlock command signal from the portable apparatus 3 which were answered and transmitted to the request signal transmitted to outdoor [of the vehicles 2] are received, the vehicle control part 13 will carry out drive controlling of the door lock drive device 22, and will perform lock/unlock control of a door lock. However, when the ID code signal from the portable apparatus 3 answered and transmitted to the request signal transmitted to the interior of a room of the vehicles 2 is received, the vehicle control part 13 will not be in an engine start authorized state. For this reason, even if a start switch is operated, the vehicle control part 13 will not control Engine control section 23. That is, although the vehicle control part 13 performs lock/unlock of a door lock when communication with the portable apparatus 3 is materialized, it forbids about engine start up. If it puts in another way, and a function restriction signal is inputted, the vehicle control part 13 will restrict security releasing operation.

[0066]

(b-2) When the ID code is contained in the function restriction signal

Also in this case, if the ID code signal from the portable apparatus 3 and the lock/unlock command signal from the portable apparatus 3 which were answered and transmitted to the request signal transmitted to outdoor [of the vehicles 2] are received, the vehicle control part 13 will carry out drive controlling of the door lock drive device 22, and will perform lock/unlock control of a door lock. That is, the vehicle control part 13 performs lock/unlock control of a door lock like the time of the ID code not being contained in the function restriction signal here. However, when the ID code signal from the portable apparatus 3 answered and transmitted to the request signal transmitted to the interior of a room of the vehicles 2 is received after the function restriction signal containing an ID code was inputted. The vehicle control part 13 compares the ID code with which the ID code first contained in this ID code signal is contained in a function restriction signal. As a result, it will restrict, when the ID code contained in an ID code signal is in agreement with the ID code contained in a function restriction signal, and the vehicle control part 13 will not be in an engine start authorized state. That is, although lock/unlock of a door lock is performed

when communication with the portable apparatus 3 with which the vehicle control part 13 corresponds with the ID code contained in a function restriction signal in this case is materialized, it forbids about engine start up. If it puts in another way and the function restriction signal containing an ID code will be inputted, the vehicle control part 13 will restrict only the security releasing operation based on communication with this ID code and the corresponding portable apparatus 3. Therefore, the vehicle control part 13 performs security releasing operation as usual, when the ID code signal and lock/unlock command signal containing other ID codes (ID code which is not contained in the functional limiting signal) recorded on the memory 13a are received. That is, only the security releasing operation using the specific portable apparatus 3 is restricted here.

[0067]

When the restriction release signal which shows that restriction control is canceled is inputted, the vehicle control part 13 cancels such function restriction control, and switches to the usual security control mode. For this reason, if input into the cellular phone 4 the restriction release number which turns into a restriction release signal, for example, communication between the cellular phone 4, the controlling device 30, and the security control device 10 is made to perform and the security control device 10 is made to receive this restriction release signal, it will switch to the usual security control mode.

[0068]

Next, in the security control system 1 for vehicles of this embodiment, the communication mode at the time of the car registration control which registers the vehicle information of the vehicles 2 into the controlling device 30, and sets up the vehicles 2 as an administration object of the controlling device 30 is explained using the sequence chart shown in drawing 2.

[0069]

As shown in the figure, registration of the vehicles 2 to the controlling device 30 is performed by communication between the security control device 10 and the controlling device 30.

In detail, first, the security control device 10 will switch to car registration mode, if transition operation to car registration mode is performed by the mode switch 21 (Step S1). Here, if the password for function restrictions is inputted from said input device (Step S2), the security control device 10 will transmit the car registration signal containing the vehicle information and the password cord for function restrictions of the vehicles 2 to the controlling device 30 (Step S3).

[0070]

If the car registration signal from the security control device 10 is received, the controlling device 30 will record the vehicle information and the password cord for function restrictions which are contained in this car registration signal on the memory 32a, and will complete registration (administrative vehicle registration) of the vehicles 2 used as an administration object (step S4). For this reason, the security control device 10 (vehicles 2) is registered

into the controlling device 30 as an administration object. And the controlling device 30 transmits the car registration completion signal which shows that car registration was completed to the security control device 10 (Step S5).

[0071]

The security control device 10 will notify the purport of registration completion by displaying that registration of the vehicles 2 was completed on a vehicle interior indicator, if the car registration completion signal from the controlling device 30 is received (Step S6). For this reason, recognition of a user is certainly attained [that registration of the vehicles 2 was completed, and] by recognizing this indicator visually.

[0072]

Next, in the security control system 1 for vehicles of this embodiment, the communication mode at the time of the ID registration control which registers the ID code of the portable apparatus 3 into the security control device 10 is explained using the sequence chart shown in drawing 3.

[0073]

As shown in the figure, it is performed by communication between the portable apparatus 3, the security control device 10, and the controlling device 30 at the time of ID registration control.

First, if the mode switch 21 of the security control device 10 is operated by the user (Step S11), the security control device 10 will switch from security control mode to ID registration mode (Step S12). If it switches to ID registration mode, the security control device 10 will transmit said request signal to the interior of a room of the vehicles 2 (Step S13).

[0074]

And the portable apparatus 3 will transmit said ID code signal, if this request signal is received (Step S14).

The security control device 10 will record the ID code contained in this ID code signal on the memory 13a, if the ID code signal from the portable apparatus 3 is received (Step S15). That is, the security control device 10 registers the ID code of the acquired portable apparatus 3 into self. Subsequently, the security control device 10 transmits said registered signal to the controlling device 30 (Step S16).

[0075]

The controlling device 30 will record the ID code contained in this registered signal on vehicle information and corresponding ID record section in the memory 32a, if the registered signal from the security control device 10 is received (Step S17). The controlling device 30 transmits said registration completion signal to the security control device 10 (Step S18). For this reason, the controlling device 30 becomes manageable [the portable apparatus 3 corresponding to the vehicles 2] based on the recorded ID code.

[0076]

If the registration completion signal from the controlling device 30 is received, the security control device 10 will perform the display which shows the purport of registration completion

to the indicator which was formed in the interior of a room of the vehicles 2, and which is not illustrated, or will perform sound information which shows the purport of this registration completion from the loudspeaker etc. which are not illustrated (Step S19). For this reason, recognition of a user is certainly attained [that registration of the portable apparatus 3 was completed, and].

[0077]

Next, in the security control system 1 for vehicles of this embodiment, the communication mode at the time of the function restriction control which forbids or restricts security releasing operation is explained using the sequence chart shown in drawing 4.

[0078]

As shown in the figure, function restriction control is performed by communication between the security control device 10, the controlling device 30, and the cellular phone 4.

In detail, first, the cellular phone 4 will transmit said restriction requirement signal containing the password cord for function restrictions to the controlling device 30, if said restriction operation is performed and the password for function restrictions is inputted (Step S21) (Step S22). Here, the cellular phone 4 transmits the restriction requirement signal containing the password cord for function restrictions, and a portable apparatus designation code to the controlling device 30, when a portable apparatus designation number is inputted with the password for function restrictions.

[0079]

The controlling device 30 specifies the corresponding vehicles 2 based on the password cord for function restrictions contained in this restriction requirement signal, if a restriction requirement signal is inputted (Step S23). And the controlling device 30 transmits said function restriction signal containing a function restriction code to the security control device 10 formed in the specified vehicles 2 (Step S24). Here, the controlling device 30 transmits the function restriction signal containing this portable apparatus designation code, a corresponding ID code, and a function restriction code, when the restriction requirement signal containing a portable apparatus designation code is inputted.

[0080]

The security control device 10 will transmit a restriction completion signal to the controlling device 30, if a function restriction signal is inputted from the controlling device 30 (Step S25). The security control device 10 performs function restriction processing shown in the above <a> or <b> (Step S26).

[0081]

The controlling device 30 will transmit the restriction completion signal to the cellular phone 4, if a restriction completion signal is received (Step S27). That is, the controlling device 30 functions as a communication relay means for transmitting the restriction completion signal transmitted from the security control device 10 to the cellular phone 4.

[0082]

And the cellular phone 4 will report to a user that the security control device 10 is in a

function restriction state by a sound, vibration, display, etc., if a restriction completion signal is received.

Therefore, according to this embodiment, the following effects can be acquired.

[0083]

(1) If the restriction requirement signal transmitted from the portable transmitter machine (cellular phone 4) possessed by the user is received by the controlling device 30, a function restriction signal will be transmitted from the controlling device 30 to the security control device 10. The security control device 10 forbids or restricts control of the door lock drive device 22 or Engine control section 23, on condition that the function restriction signal was received. That is, the security control device 10 forbids or restricts the security releasing operation by security equipments on condition of reception of this function restriction signal. For this reason, when a user loses the portable apparatus 3 or a theft is carried out, the security releasing operation by the security control device 10 can be forbidden or restricted by making a restriction requirement signal transmit from the cellular phone 4. Therefore, also in the time of loss and the theft of the portable apparatus 3, the security releasing operation by this portable apparatus 3 can be forbidden or restricted immediately, and the high security level of security equipments can be secured.

[0084]

(2) Since the security releasing operation using this portable apparatus 3 will be simply forbidden or restricted by the user even if a third party does the theft of the portable apparatus 3, worth of portable apparatus 3 after a theft falls substantially. Even mind that a third party is going to do the theft of the portable apparatus 3 stops therefore, boiling. That is, the volition of the theft of the portable apparatus 3 by a third party itself can be made to decline, and the anti-theft nature of the portable apparatus 3 also improves.

[0085]

(3) If the portable apparatus designation number which specifies the portable apparatus 3 is inputted by the user when the cellular phone 4 performs restriction operation, the security control device 10 will forbid or restrict only the security release based on communication with the this specified portable apparatus 3. That is, if the portable apparatus 3 which should be restricted is specified when the cellular phone 4 performs restriction operation, only the security release by the specific portable apparatus 3 can be made to forbid or restrict. For this reason, when the portable apparatus 3 is lost, for example or a theft is carried out, only the security release by that portable apparatus 3 can be forbidden or restricted, and a passage becomes usually possible about the security release by the portable apparatus 3 registered into others. That is, about the portable apparatus 3 by which is lost or a theft is not carried out, it becomes available, without receiving restriction in any way. Therefore, even the security release by the portable apparatus 3 which does not need function restriction cannot be forbidden or restricted, and the convenience of the portable apparatus 3 can be secured.

[0086]

The embodiment of this invention may be changed as follows.
- state **** by which the security control device 10 is set as the 1st function restriction processing (security release prohibition process) -- when the function restriction signal which does not contain the ID code is received (in the case of the above (a-1)), the communication with the portable apparatus 3 itself is forbidden. If it changes in this way and a function restriction signal will be inputted into the vehicle control part 13, communication with the security control device 10 and the portable apparatus 3 in security control mode will become impossible. Therefore, communication with the portable apparatus 3 and the vehicle control part 13 stops materializing, and control of the door lock drive device 22 by the vehicle control part 13 and Engine control section 23 is forbidden certainly. Therefore, the high security level of security equipments is securable. And if the security control device 10 receives a function restriction signal in this case, a request signal will not be transmitted at the time of security control mode. The portable apparatus 3 will not transmit an ID code signal in order not to receive a request signal. Therefore, the useless communication between the portable apparatus 3 and the security control device 10 can be prevented, and the power consumption of the portable apparatus 3 and the security control device 10 can be reduced.

[0087]
- In the aforementioned embodiment, the controlling device 30 transmits a function restriction signal to the security control device 10. However, the portable apparatus side communications department 44 in which the controlling device 30 and communication are possible is established in the portable apparatus 3, and it may be made to, make this function restriction signal transmit to drawing 1 from the controlling device 30 to the portable apparatus 3, as a two-dot chain line shows for example. And at the time of communication with the security control device 10 after the portable apparatus 3 receives this function restriction signal in this case, it changes so that the sending signal (an ID code signal, a lock/unlock command signal) containing a function restriction code may be made to transmit from the portable apparatus 3. On the other hand, when the security control device 10 receives the sending signal containing this function restriction code, the security control device 10 is changed so that control which forbids or restricts security control operation may be performed. Even if it does in this way, at the time of loss and the theft of the portable apparatus 3, the security releasing operation which used this portable apparatus 3 is forbidden or restricted certainly. Therefore, the high security level of security equipments is securable.

[0088]
An ID code signal and a lock/unlock command signal cannot be transmitted for the portable apparatus 3 which received the function restriction signal.
- when the security control device 10 receives a function restriction signal, it performs prohibition or restriction for the security releasing operation based on communication with the portable apparatus 3 -- in addition, said ID registration control is forbidden by ceasing to

switch to ID registration mode. If it does in this way, the security releasing operation using the portable apparatus 3 which newly tried registration will be forbidden certainly. Therefore, unjust registration of the ID code by a third party can be prevented, and it becomes possible to secure the high security level of security equipments.

[0089]

- According to the aforementioned embodiment, if the security control device 10 will be in a function restriction state, it will transmit the restriction completion signal which shows that to the cellular phone 4 via the controlling device 30. However, a restriction completion signal is directly transmitted from the security control device 10 by a telephone line etc. via the controlling device 30 to the cellular phone 4.

[0090]

- According to the aforementioned embodiment, the cellular phone 4 is notified that the security control device 10 changed into the function restriction state by transmitting a restriction completion signal to the cellular phone 4 via the controlling device 30 from the security control device 10. However, when the controlling device 30 transmits a function restriction signal to the security control device 10, it may change so that a restriction completion signal may be transmitted to the cellular phone 4 from this controlling device 30. That is, in this case, the controlling device 30 has having transmitted the function restriction signal in the security control device 10, judges that this security control device 10 changed into the function restriction state, and notifies that to the cellular phone 4.

[0091]

- The mutual recognition (pairing) for judging whether each is operating normally between the vehicle control part 13 of the security control device 10 and the security communication part 14 may be made to perform in the aforementioned embodiment. And when it is judged that each is operating normally (i.e., only when this mutual recognition is materialized), it is good also as registration to the security control device 10 being possible in the ID code of the portable apparatus 3. Since the mutual recognition between both will not be materialized when the security communication part 14 is removed unjustly or is destroyed, for example if it does in this way, it cannot register with the security control device 10. Therefore, unjust registration of an ID code can be prevented more certainly.

[0092]

- A GPS module is provided in the portable apparatus 3, the position of the portable apparatus 3 is recognized with the controlling device 30 at the time of function restriction, and it may be made to notify the position of this portable apparatus 3 to the cellular phone 4 from the controlling device 30. If it does in this way, the user can recognize certainly the whereabouts of the portable apparatus 3 by which was lost or the theft was carried out.

[0093]

- According to the aforementioned embodiment, a restriction requirement signal is transmitted from the cellular phone 4 to the controlling device 30. However, restriction operation by a user is enabled by the vehicles 2, and it is good from the security control

device 10 also considering a restriction requirement signal as ability ready for sending to the controlling device 30. That is, it is good by performing restriction operation by the vehicles 2 also as possible in the function restriction of security equipments (the door lock drive device 22 and Engine control section 23). If it does in this way, when performing function restriction, portable transmitter machines, such as the cellular phone 4, become unnecessary.

[0094]

- Make a car registration signal transmit to the controlling device 30 from the security control device 10 in each aforementioned embodiment at the time of the car registration control for setting up the vehicles 2 as an administration object of the controlling device 30. However, at the time of such car registration control, the security control device 10 is good for the controlling device 30 also considering said car registration signal as ability ready for sending from the registration device formed independently. For example, it is good for the controlling device 30 also considering a car registration signal as ability ready for sending from this personal computer, using a personal computer as a registration device. In this case, car registration information, including vehicle information, the password for function restrictions, etc., is inputted into a personal computer, and it is made to make a car registration signal including this car registration information transmit to the controlling device 30 via communications networks, such as the Internet. Since it will necessarily be [the security control device 10 (vehicles 2)] less necessary for car registration work if it does in this way, the convenience of this car registration work improves. If the password set up by the user, the dealer, the maker of the portable apparatus 3, etc. is given to a car registration signal, the unjust car registration by a third party can be prevented.

[0095]

The work (car registration work) which registers the vehicles 2 into the controlling device 30 and the work (ID registration work) which registers the ID code of the portable apparatus 3 into the security control device 10, It is carried out by workers who can trust it for a user, such as not only a user but a dealer, and a maker of the portable apparatus 3.

[0096]

- In the aforementioned embodiment, the wire communication for which the communication between the security control device 10 and the controlling device 30 used the public network in addition to radio, for example may be adopted. For example, the end connection to which the modular jack of a telephone is connected is provided in the vehicles 2, and it may be made to perform communication with the security control device 10 and the controlling device 30 using a telephone wire.

[0097]

- Not only the cellular phone 4 but in each aforementioned embodiment, portable transmitter machines may be a personal computer of a note type, PDA (Personal Digital Assistance : Personal Digital Assistant), communication equipment for exclusive use, etc., for example.

[0098]
- The security control system 1 for vehicles of each aforementioned embodiment is provided with the following.
The function in which a door lock is automatically unlocked by the two-way communication of the portable apparatus 3 and the security control device 10 because the portable apparatus 3 approaches the vehicles 2 (smart entry function).
The function in which engine start up is permitted because the portable apparatus 3 advances into the interior of a room of the vehicles 2 (smart ignition function).
However, the security control system 1 for vehicles does not need to be provided with such a smart entry function or smart ignition function. For example, when the portable apparatus 3 is provided with a transponder and a machinery key and equips the vehicles 2 with this machinery key, it performs two-way communication with the security control device 10. And on condition that rotating operation of this machinery key was carried out, it controls the door lock drive device 22 and Engine control section 23, while permitting the rotating operation of a machinery key, when the security control device 10 is materialized [two-way communication with this transponder]. That is, the security control device 10 should just perform security releasing operation based on two-way communication with the portable apparatus 3.
[0099]
It may not be indispensable about the two-way communication of such the portable apparatus 3 and the security control device 10, either. For example, it may be ability ready for sending only about said lock/unlock command signal, and the security control device 10 is not provided with the sending circuit 11 with it, but the portable apparatus 3 may be constituted so that a request signal may not be transmitted. That is, if the security control device 10 is coming to perform security releasing operation based on communication with the portable apparatus 3, two-way communication with the portable apparatus 3 will not necessarily be performed.
[0100]
- In the aforementioned embodiment, the controlling device 30 manages the number of the ID codes of the portable apparatus 3 which can be registered into the security control device 10 formed in the vehicles 2 used as an administration object. However, the controlling device 30 does not necessarily manage the number of these ID codes.
[0101]
The controlling device 30 does not necessarily need to manage the ID code of the portable apparatus 3. That is, the controlling device 30 does not necessarily record an ID code on the memory 32a. If it does in this way, while the record burden of the memory 32a of the controlling device 30 is mitigable, between the security control device 10 and the controlling device 30, it becomes unnecessary to perform transmission and reception of a registered signal or a registration completion signal, and both communication burden can be eased. It becomes impossible however, to make the control (control shown in the above (a-2) and (b-

2)) to which only the security releasing operation by the predetermined portable apparatus 3 is made to forbid or restrict in this case perform to the security control device 10.

[0102]

Then, if it is in such an example of change, the controlling device 30 may be changed so that the function restriction signal containing the portable apparatus designation code may be transmitted to the security control device 10, when the restriction requirement signal which contains a portable apparatus designation code, for example is received. And the registration number corresponding to the ID code recorded on the memory 13a of the security control device 10 with a portable apparatus designation code may be given. If it does in this way, the security control device 10 can forbid or restrict only the security releasing operation by communication with the predetermined portable apparatus 3 based on the portable apparatus designation code contained in a function restriction signal, and the registration number recorded on the memory 13a.

[0103]

- If the security control system 1 for vehicles switches even the security control device 10 to ID registration mode in each aforementioned embodiment, registration of the portable apparatus 3 is possible anywhere. However, a GPS module is connected to the security control device 10, for example, The security control system 1 for vehicles may be changed so that the registration of the portable apparatus 3 of the security control device 10 may be attained only at the predetermined places (for example, a house, a company, a dealer, etc.) set up beforehand. If it does in this way, unjust registration of the ID code by a third party can be prevented further, and the security level of security equipments can be raised further. Such a change may be similarly limited for the place in which the car registration which registers not only the registration office of the portable apparatus 3 but the vehicles 2 as an administration object of the controlling device 30 is possible.

[0104]

- In the aforementioned embodiment, the operation for switching the security control device 10 to ID registration mode is not limited to operation of the mode switch 21. For example, the existing switches (for example, lever combination switch etc.) with which the security control device 10 was formed in the vehicles 2, It may be changed so that it may switch to ID registration mode in a predetermined mode (presetting by the user or a dealer of the mode which only a user and a dealer can know, etc. are desirable). If it does in this way, the mode switch 21 is omissible. A change in the ID registration mode which is not meant can be prevented by the operation mistake of the mode switch 21. The operation for switching to car registration mode may be changed similarly.

[0105]

- The aforementioned controlling device 30 may be allocated in not only a control center for exclusive use but a user's house, etc., and may be constituted by the personal computer etc. in this case.

- In said embodiment, the cellular phone 4 transmits a restriction requirement signal to the

controlling device 30, when voice input of the predetermined voice commanding is carried out.

[0106]

Communication between the cellular phone 4 and the controlling device 30 may be performed by the conversation of the operator and user who are residing at the control center in which the controlling device 30 was allocated. That is, a user telephones a control center using the cellular phone 4, and directs a restriction demand by conversation with an operator. In this case, the operator which received directions will operate the controlling device 30 based on these directions, and will perform function restriction control. If it does in this way, it will become unnecessary to make a restriction requirement signal transmit to the controlling device 30 from the cellular phone 4.

[0107]

- The door lock drive device 22 or not only Engine control section 23 but security equipments may be a steering lock device, a shift lock device, a tire locking device, etc., for example. That is, if it is a device for restricting or checking a run of the normal vehicles 2, it is applicable as security equipments.

[0108]

- A security control system may be materialized as a security system for buildings which controls the lock/unlock of the door for buildings, for example in addition to the security control system 1 for vehicles which controls the security equipments of vehicles.

[0109]

Next, the technical ideas grasped by the embodiment mentioned above are enumerated below besides the technical idea indicated to the claim.

(1) In a security control system given in any 1 paragraph of claims 1-5, when said controlling device transmits said function restriction signal to said portable apparatus or said security control device, transmit the reporting signal which shows that to the portable apparatus apparatus possessed by the user. According to the invention given in this technical idea (1), the user can recognize certainly and promptly that function restriction is carried out.

[0110]

(2) In the security control system of a statement, in claims 1-5 and any 1 paragraph of a technical idea (1) said security control device, When you perform mutual recognition of whether each is operating normally said security communication means, said control means, and in between and this mutual recognition is not materialized, forbid the security releasing operation by said security equipments based on communication with said portable apparatus. According to the invention given in this technical idea (2), since security releasing operation is forbidden when a security communication means is removed, for example or it is destroyed, unjust security releasing operation can be prevented more certainly.

[0111]

(3) To claims 1-5, a technical idea (1), and (2), in the security control system of a statement, said security control device is an object for vehicles, and said security equipments, At least one side of the Engine control sections which control the start-up permission of a door lock drive device and an engine which controls the lock/unlock of a door lock should be included.

[0112]

(4) Transmit said restriction requirement signal to said controlling device from this portable transmitter machine by operating the portable transmitter machine possessed by the user in the security control method according to claim 11.

[Brief Description of the Drawings]

[0113]

[Drawing 1]The block diagram showing the outline composition of one embodiment which materialized this invention to the security control system for vehicles.

[Drawing 2]The sequence chart which shows the communication mode at the time of car registration control.

[Drawing 3]The sequence chart which shows the communication mode at the time of ID registration control.

[Drawing 4]The sequence chart which shows the communication mode at the time of function restriction control.

[Description of Notations]

[0114]

1 [-- The cellular phone as a portable transmitter machine,] -- The security control system for vehicles, 2 -- Vehicles, 3 -- Portable apparatus, 4 10 -- A security control device, 13 -- The vehicle control part as a control means, 13a -- The memory as a recording device, 14 -- The security communication part as a security communication means, 22 [-- The management communications department, 32 / -- The supervisory control part as a restriction control means, 33 / -- The communications department for portable devices as the means of communication for portable devices, and a reception means.] -- The door lock drive device as security equipments, 23 -- The Engine control section as security equipments, 30 -- A controlling device, 31

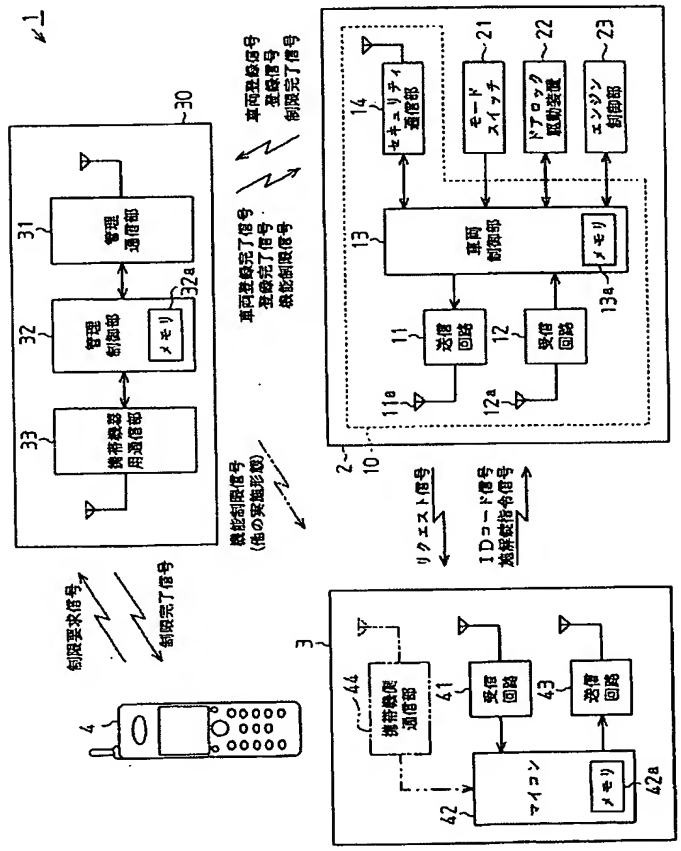
[Translation done.]

* NOTICES *

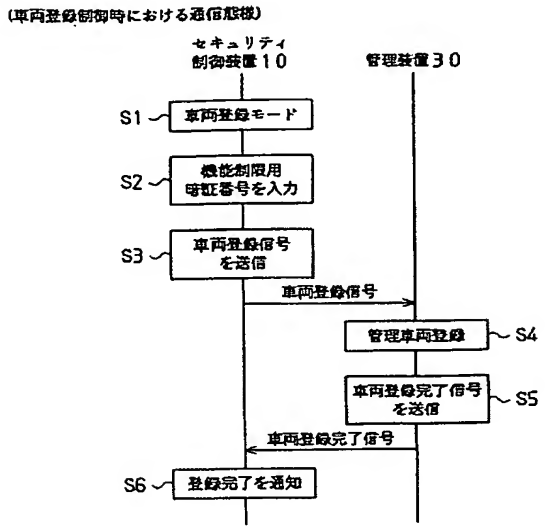
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

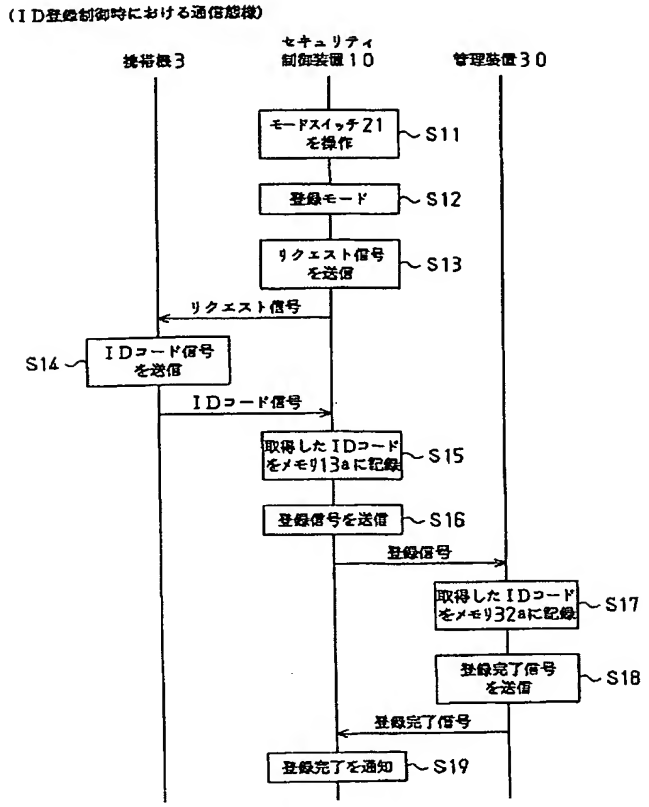
[Drawing 1]



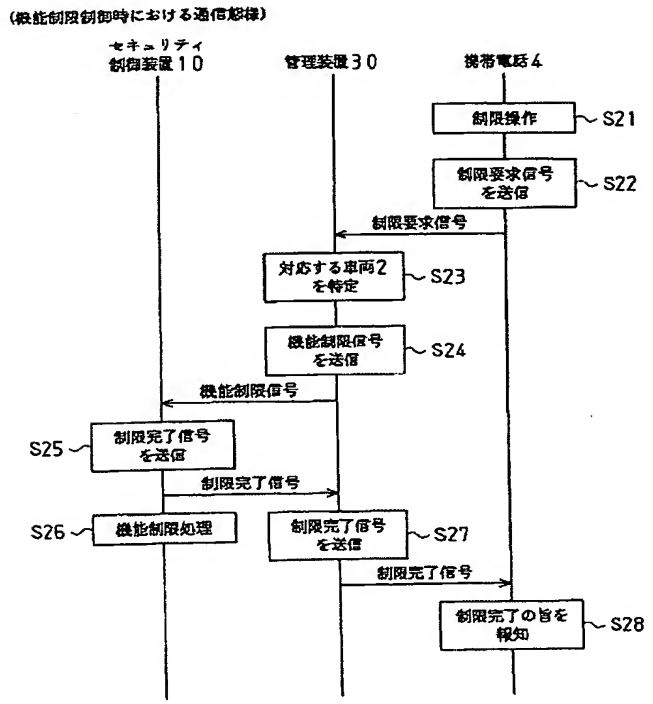
[Drawing 2]


(車両登録制御時における通信態様)
セキュリティ制御装置10
管理装置30
S1
車両登録モード
S2
機能制限用暗証番号を入力
S3
車両登録信号を送信
車両登録信号
管理車両登録
S4
車両登録完了信号を送信
S5
車両登録完了信号
S6
登録完了を通知

[Drawing 3]


（ＩＤ登録制御時における通信態様）
携帯機３
セキュリティ制御装置１０
管理装置３０
モードスイッチ21を操作
S11
登録モード
S12
リクエスト信号を送信
S13
リクエスト信号
S14
ＩＤコード信号を送信
ＩＤコード信号
取得したＩＤコードをメモリ13aに記録
S15
登録信号を送信
S16
登録信号
取得したＩＤコードをメモリ32aに記録
S17
登録完了信号を送信
S18
登録完了信号
登録完了を通知
S19

[Drawing 4]



[Translation done.]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-226390
(P2005-226390A)
(43)公開日　平成17年8月25日(2005.8.25)

(51)Int.Cl.[7]		F I			テーマコード（参考）
E05B	49/00	E05B	49/00	K	2E250
B60R	25/00	B60R	25/00	606	5K011
B60R	25/10	B60R	25/10	617	5K067
H04B	1/38	H04B	1/38		
H04Q	7/38	H04B	7/26	109R	

審査請求 未請求　請求項の数 11　OL　（全 22 頁）

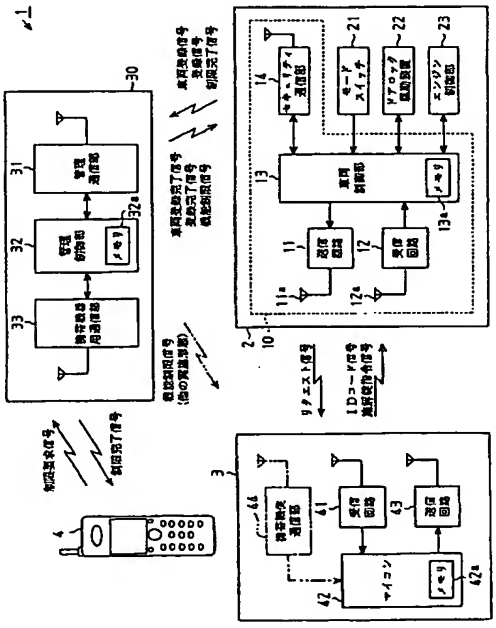
(21)出願番号　特願2004-38023(P2004-38023)
(22)出願日　平成16年2月16日(2004.2.16)

(71)出願人　000003551
株式会社東海理化電機製作所
愛知県丹羽郡大口町豊田三丁目２６０番地
(71)出願人　000003207
トヨタ自動車株式会社
愛知県豊田市トヨタ町１番地
(74)代理人　100068755
弁理士　恩田　博宣
(74)代理人　100105957
弁理士　恩田　誠
(72)発明者　河村　大輔
愛知県丹羽郡大口町豊田三丁目２６０番地
株式会社東海理化電機製作所内

最終頁に続く

(54)【発明の名称】セキュリティ制御システム、セキュリティ制御装置、セキュリティ制御システムにおける管理装置、及び、セキュリティ制御方法

(57)【要約】
【課題】　セキュリティ機器のセキュリティレベルをより一層向上させることができるセキュリティ制御システム、セキュリティ制御装置、セキュリティ制御システムにおける管理装置、及び、セキュリティ制御方法を提供する。
【解決手段】　セキュリティ制御装置１０は、携帯機３との通信により、携帯機３に設定されたＩＤコードとメモリ１３ａに既に記録されているＩＤコードとの照合を行い、該照合の成立の有無に基づいてドアロック駆動装置２２やエンジン制御部２３を制御する。また、管理装置３０は、携帯電話４から制限要求信号が入力されたことを条件として、セキュリティ制御装置１０に機能制限信号を送信する。そして、セキュリティ制御装置１０は、該機能制限信号を受信すると、携帯機３との通信に基づくセキュリティ機器（ドアロック駆動装置２２、エンジン制御部２３）の制御を禁止または制限する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
通信機能を有する携帯機と、該携帯機に設定されたＩＤコードと自身の記録手段に既に記録されているＩＤコードとの照合を該携帯機との通信に基づいて行うとともに、その照合結果に基づいてセキュリティ機器を制御することにより、該セキュリティ機器によるセキュリティ解除動作を制御するセキュリティ制御装置と、該セキュリティ制御装置との通信を行う管理装置とを備えたセキュリティ制御システムであって、
前記管理装置は、制限要求信号が入力されたことを条件として、前記携帯機及び前記セキュリティ制御装置の少なくとも一方に機能制限信号を送信し、
前記セキュリティ制御装置は、前記機能制限信号を受信した際における前記携帯機との通信、または前記機能制限信号を受信した前記携帯機との通信に基づく前記セキュリティ機器の制御を禁止または制限することを特徴とするセキュリティ制御システム。
【請求項２】
前記セキュリティ制御装置は、前記機能制限信号を受信した際には、前記携帯機との通信自体を禁止することを特徴とする請求項１に記載のセキュリティ制御システム。
【請求項３】
前記携帯機は、前記機能制限信号を受信した際には、前記セキュリティ制御装置との通信時に、機能制限コードを含む送信信号を送信し、
前記セキュリティ制御装置は、前記送信信号を受信したことを条件として、前記セキュリティ機器の制御を禁止または制限することを特徴とする請求項１または請求項２に記載のセキュリティ制御システム。
【請求項４】
前記制限要求信号は、前記携帯機とは別にユーザによって所持される携帯通信機器から送信され、
前記管理装置は、前記制限要求信号を受信する受信手段を備え、該受信手段を介して前記制限要求信号が入力されたことを条件として前記機能制限信号を送信することを特徴とする請求項１～３のいずれか１項に記載のセキュリティ制御システム。
【請求項５】
前記セキュリティ制御装置は、前記携帯機に設定されたＩＤコードを前記記録手段に記録するＩＤ登録制御を該携帯機との通信に基づいて行う一方、前記機能制限信号を受信した際における前記携帯機との通信、または前記機能制限信号を受信した前記携帯機との通信時には、該ＩＤ登録制御を禁止することにより、該携帯機との通信に基づく前記セキュリティ機器の制御を禁止することを特徴とする請求項１～４のいずれか１項に記載のセキュリティ制御システム。
【請求項６】
固有のＩＤコードが設定された携帯機との通信を行う携帯機用通信手段と、
前記ＩＤコードと対応するＩＤコードが記録される記録手段と、
前記携帯機との通信時に、携帯機に設定されたＩＤコードと前記記録手段に記録されたＩＤコードとの照合を行い、該照合が一致したか否かに基づいてセキュリティ機器を制御するセキュリティ制御手段と、
当該セキュリティ制御装置の外部に配設される管理装置と通信可能なセキュリティ通信手段と、を備え、
前記セキュリティ制御手段は、前記管理装置から送信される機能制限信号を前記セキュリティ通信手段によって受信したことを条件として、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限することを特徴とするセキュリティ制御装置。
【請求項７】
前記セキュリティ制御手段は、前記機能制限信号を前記セキュリティ通信手段によって受信した際には、前記携帯機との通信自体を禁止することを特徴とする請求項６に記載のセキュリティ制御装置。
【請求項８】

前記セキュリティ制御手段は、前記携帯機に設定されたＩＤコードを前記記録手段に記録するＩＤ登録制御を該携帯機との通信に基づいて行う一方、前記機能制限信号を前記セキュリティ通信手段によって受信した際には、該ＩＤ登録制御を禁止することにより、該携帯機との通信に基づく前記セキュリティ機器の制御を禁止または制限することを特徴とする請求項６または請求項７に記載のセキュリティ制御装置。

【請求項９】

通信機能を有する携帯機との通信に基づき、該携帯機に設定されたＩＤコードと自身に予め登録されたＩＤコードとの照合結果に基づいてセキュリティ機器を制御するセキュリティ制御装置と通信可能な管理通信手段、及び、前記携帯機と通信可能な携帯機用通信手段のうちの少なくとも一方と、

制限要求信号が入力されたことを条件として、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限させるための機能制限信号を、前記管理通信手段または前記携帯機用通信手段を介して、前記セキュリティ制御装置及び前記携帯機のうちの少なくとも一方に送信する制限制御手段とを備えることを特徴とするセキュリティ制御システムにおける管理装置。

【請求項１０】

ユーザによって所持される携帯通信機器との通信を行う携帯機器用通信手段を備え、

該携帯機器用通信手段は、前記携帯通信機器から送信される制限要求信号を受信し、その制限要求信号を前記制限制御手段に入力することを特徴とする請求項９に記載のセキュリティ制御システムにおける管理装置。

【請求項１１】

通信機能を有する携帯機との通信により、携帯機に設定されたＩＤコードと自身の記録手段に既に記録されているＩＤコードとの照合を行うとともに、その照合結果に基づいてセキュリティ機器を制御することにより、該セキュリティ機器によるセキュリティ解除動作を制御するセキュリティ制御装置と、該セキュリティ制御装置との通信を行う管理装置とを備えたセキュリティ制御システムにおけるセキュリティ制御方法であって、

前記管理装置に対してユーザから機能制限を行う旨の制限要求信号が入力された際に、該管理装置から前記携帯機または前記セキュリティ制御装置の少なくとも一方に対して機能制限信号を送信し、

前記セキュリティ制御装置が前記機能制限信号を受信した際における前記携帯機との通信時、または前記機能制限信号を受信した前記携帯機との通信時には、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限させることを特徴とするセキュリティ制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、例えば車両や住宅などに用いられるセキュリティ制御システム、セキュリティ制御装置、該セキュリティ制御システムにおける管理装置、及び、セキュリティ制御方法に関するものである。

【背景技術】

【０００２】

一般に、車両や住宅のドア錠装置などのセキュリティ機器は、ユーザによって所持される専用の機械キーを用いて操作可能となっている。しかし、この場合、機械キーが不正にコピーされたり、ピッキングなどが行われたりすることにより、セキュリティ機器が不正に操作されてしまうおそれがあるため、社会的に問題視されている。

【０００３】

そこで従来、セキュリティ機器のセキュリティレベルの向上を図るために、例えば電子照合を用いたセキュリティ制御システムが提案されている（例えば、特許文献１、特許文献２参照）。

【０００４】

これら特許文献１，２に示されるように、例えば車両用セキュリティ制御システムでは、ユーザによって所持される携帯機と、車両に配設されたセキュリティ制御装置との間で無線通信が行われる。具体的には、携帯機に設定された固有のＩＤコードを含むＩＤコード信号が携帯機からセキュリティ制御装置に送信されると、セキュリティ制御装置は、該ＩＤコード信号に含まれるＩＤコードと、自身に予め登録されているＩＤコードとの比較を行う。そして、セキュリティ制御装置は、それらＩＤコード同士が一致した際に携帯機との通信が成立したと判断し、ドア錠を解錠させたりエンジンの始動許可を行ったりするようになっている。すなわち、セキュリティ制御装置は、携帯機との通信が成立したことを条件として、各種セキュリティ機器のセキュリティ解除動作を行うようになっている。このため、対応する携帯機を所持しない第三者によるセキュリティ解除動作が不能となり、セキュリティレベルが向上する。

【特許文献１】特開２００１－２８９１４２号公報
【特許文献２】特開２００１－３１１３３３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、従来の車両用セキュリティ制御装置では、通常の使用状態においては優れた盗難防止効果を得ることができるものの、ユーザが携帯機を紛失したり、該携帯機を盗難されたりした場合には、第三者によって該携帯機が使用されてしまうおそれがある。このように、従来の車両用セキュリティ制御システムにおいては、特殊なケースではあるものの、万全の盗難防止効果が得られない場合がある。
【０００６】
そこで従来では、セキュリティ機器のセキュリティレベルをより一層高くすることが要望されている。
本発明はこうした実情に鑑みてなされたものであり、その目的は、セキュリティ機器のセキュリティレベルをより一層向上させることができるセキュリティ制御システム、セキュリティ制御装置、セキュリティ制御システムにおける管理装置、及び、セキュリティ制御方法を提供することにある。
【課題を解決するための手段】
【０００７】
上記の課題を解決するために、請求項１に記載の発明では、通信機能を有する携帯機と、該携帯機に設定されたＩＤコードと自身の記録手段に既に記録されているＩＤコードとの照合を該携帯機との通信に基づいて行うとともに、その照合結果に基づいてセキュリティ機器を制御することにより、該セキュリティ機器によるセキュリティ解除動作を制御するセキュリティ制御装置と、該セキュリティ制御装置との通信を行う管理装置とを備えたセキュリティ制御システムであって、前記管理装置は、制限要求信号が入力されたことを条件として、前記携帯機及び前記セキュリティ制御装置の少なくとも一方に機能制限信号を送信し、前記セキュリティ制御装置は、前記機能制限信号を受信した際における前記携帯機との通信、または前記機能制限信号を受信した前記携帯機との通信に基づく前記セキュリティ機器の制御を禁止または制限することを要旨とする。
【０００８】
請求項２に記載の発明では、請求項１に記載のセキュリティ制御システムにおいて、前記セキュリティ制御装置は、前記機能制限信号を受信した際には、前記携帯機との通信自体を禁止することを要旨とする。
【０００９】
請求項３に記載の発明では、請求項１または請求項２に記載のセキュリティ制御システムにおいて、前記携帯機は、前記機能制限信号を受信した際には、前記セキュリティ制御装置との通信時に、機能制限コードを含む送信信号を送信し、前記セキュリティ制御装置は、前記送信信号を受信したことを条件として、前記セキュリティ機器の制御を禁止または制限することを要旨とする。

【００１０】
請求項４に記載の発明では、請求項１～３のいずれか１項に記載のセキュリティ制御システムにおいて、前記制限要求信号は、前記携帯機とは別にユーザによって所持される携帯通信機器から送信され、前記管理装置は、前記制限要求信号を受信する受信手段を備え、該受信手段を介して前記制限要求信号が入力されたことを条件として前記機能制限信号を送信することを要旨とする。
【００１１】
請求項５に記載の発明では、請求項１～４のいずれか１項に記載のセキュリティ制御システムにおいて、前記セキュリティ制御装置は、前記携帯機に設定されたＩＤコードを前記記録手段に記録するＩＤ登録制御を該携帯機との通信に基づいて行う一方、前記機能制限信号を受信した際における前記携帯機との通信、または前記機能制限信号を受信した前記携帯機との通信時には、該ＩＤ登録制御を禁止することにより、該携帯機との通信に基づく前記セキュリティ機器の制御を禁止することを要旨とする。
【００１２】
請求項６に記載の発明では、固有のＩＤコードが設定された携帯機との通信を行う携帯機用通信手段と、前記ＩＤコードと対応するＩＤコードが記録される記録手段と、前記携帯機との通信時に、携帯機に設定されたＩＤコードと前記記録手段に記録されたＩＤコードとの照合を行い、該照合が一致したか否かに基づいてセキュリティ機器を制御するセキュリティ制御手段と、当該セキュリティ制御装置の外部に配設される管理装置と通信可能なセキュリティ通信手段と、を備え、前記セキュリティ制御手段は、前記管理装置から送信される機能制限信号を前記セキュリティ通信手段によって受信したことを条件として、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限することを要旨とする。
【００１３】
請求項７に記載の発明では、請求項６に記載のセキュリティ制御装置において、前記セキュリティ制御手段は、前記機能制限信号を前記セキュリティ通信手段によって受信した際には、前記携帯機との通信自体を禁止することを要旨とする。
【００１４】
請求項８に記載の発明では、請求項６または請求項７に記載のセキュリティ制御装置において、前記セキュリティ制御手段は、前記携帯機に設定されたＩＤコードを前記記録手段に記録するＩＤ登録制御を該携帯機との通信に基づいて行う一方、前記機能制限信号を前記セキュリティ通信手段によって受信した際には、該ＩＤ登録制御を禁止することにより、該携帯機との通信に基づく前記セキュリティ機器の制御を禁止または制限することを要旨とする。
【００１５】
請求項９に記載の発明では、通信機能を有する携帯機との通信に基づき、該携帯機に設定されたＩＤコードと自身に予め登録されたＩＤコードとの照合結果に基づいてセキュリティ機器を制御するセキュリティ制御装置と通信可能な管理通信手段、及び、前記携帯機と通信可能な携帯機用通信手段のうちの少なくとも一方と、制限要求信号が入力されたことを条件として、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限させるための機能制限信号を、前記管理通信手段または前記携帯機用通信手段を介して、前記セキュリティ制御装置及び前記携帯機のうちの少なくとも一方に送信する制限制御手段とを備えることを要旨とする。
【００１６】
請求項１０に記載の発明では、請求項９に記載のセキュリティ制御システムにおける管理装置において、ユーザによって所持される携帯通信機器との通信を行う携帯機器用通信手段を備え、該携帯機器用通信手段は、前記携帯通信機器から送信される制限要求信号を受信し、その制限要求信号を前記制限制御手段に入力することを要旨とする。
【００１７】
請求項１１に記載の発明では、通信機能を有する携帯機との通信により、携帯機に設定

されたＩＤコードと自身の記録手段に既に記録されているＩＤコードとの照合を行うとともに、その照合結果に基づいてセキュリティ機器を制御することにより、該セキュリティ機器によるセキュリティ解除動作を制御するセキュリティ制御装置と、該セキュリティ制御装置との通信を行う管理装置とを備えたセキュリティ制御システムにおけるセキュリティ制御方法であって、前記管理装置に対してユーザから機能制限を行う旨の制限要求信号が入力された際に、該管理装置から前記携帯機または前記セキュリティ制御装置の少なくとも一方に対して機能制限信号を送信し、前記セキュリティ制御装置が前記機能制限信号を受信した際における前記携帯機との通信時、または前記機能制限信号を受信した前記携帯機との通信時には、前記セキュリティ機器によるセキュリティ解除動作を禁止または制限させることを要旨とする。

【００１８】

以下、本発明の「作用」について説明する。

請求項１，１１に記載の発明によると、制限要求信号が管理装置によって受信されると、該管理装置から携帯機及びセキュリティ制御装置のうちの少なくとも一方に対して機能制限信号が送信される。そして、セキュリティ制御装置は、該機能制限信号を受信した際における携帯機との通信や、該機能制限信号を受信した携帯機との通信に基づくセキュリティ機器の制御を禁止または制限する。このため、ユーザが携帯機を紛失したり盗難されたりした場合には、管理装置に制限要求信号を入力する措置を施すことにより、セキュリティ制御装置によるセキュリティ解除動作を禁止または制限することができる。よって、携帯機の紛失・盗難時には、該携帯機を用いたセキュリティ解除動作を禁止または制限することができ、セキュリティ機器の高いセキュリティレベルを確保することができる。

【００１９】

請求項２に記載の発明によると、セキュリティ制御装置は、管理装置からの機能制限信号を受信すると、携帯機との通信自体を禁止する。すなわち、セキュリティ制御装置は、機能制限信号を受信すると、携帯機との通信に基づくセキュリティ解除動作を禁止する。このため、携帯機の紛失・盗難時には、該携帯機を用いたセキュリティ解除動作が確実に禁止される。よって、セキュリティ機器の高いセキュリティレベルを確保することが可能となる。

【００２０】

請求項３に記載の発明によると、携帯機は、機能制限信号を受信すると、セキュリティ制御装置との通信時に、機能制限コードを含む送信信号を送信する。一方、セキュリティ制御装置は、該機能制限コードを含む送信信号を受信したことを条件として、セキュリティ制御動作を禁止または制限する。このため、携帯機の紛失・盗難時には、該携帯機を用いたセキュリティ解除動作が確実に禁止または制限される。よって、セキュリティ機器の高いセキュリティレベルを確保することが可能となる。

【００２１】

請求項４に記載の発明によると、ユーザが所持する携帯通信機器から送信される制限要求信号が管理装置によって受信されると、管理装置からセキュリティ制御装置に対して機能制限信号が送信される。このため、ユーザが携帯機を紛失したり盗難されたりした場合には、携帯通信機器から制限要求信号を送信させることにより、セキュリティ解除動作を禁止または制限することができる。よって、携帯機の紛失・盗難時には、該携帯機によるセキュリティ解除動作を即座に禁止または制限することができ、セキュリティ機器の高いセキュリティレベルを確保することが可能となる。

【００２２】

請求項５に記載の発明によると、セキュリティ制御装置は、機能制限信号を受信した際における携帯機との通信、または機能制限信号を受信した携帯機との通信時には、ＩＤ登録制御を禁止する。このため、該携帯機とセキュリティ制御装置との通信が成立しなくなり、該携帯機を用いたセキュリティ解除動作が確実に禁止される。よって、第三者によるＩＤコードの不正な登録を防止することができ、セキュリティ機器の高いセキュリティレベルを確保することが可能となる。

【００２３】
請求項６に記載の発明によると、管理装置から送信される機能制限信号がセキュリティ通信手段によって受信されると、セキュリティ制御手段は、セキュリティ機器によるセキュリティ解除動作を禁止または制限する。このため、例えばユーザが携帯機を紛失したり盗難されたりした場合、ユーザによる措置により管理装置から制限要求信号を送信させるようにすれば、セキュリティ制御装置によるセキュリティ解除動作を禁止または制限することができる。よって、携帯機の紛失・盗難時には、該携帯機を用いたセキュリティ解除動作を禁止または制限することができ、セキュリティ機器の高いセキュリティレベルを確保することができる。
【００２４】
請求項７に記載の発明によると、管理装置からの機能制限信号をセキュリティ通信手段によって受信すると、セキュリティ制御手段は、携帯機との通信自体を禁止し、携帯機との通信に基づくセキュリティ解除動作を禁止する。このため、例えば携帯機の紛失・盗難時に管理装置から制限要求信号を送信させるようにすれば、該携帯機を用いたセキュリティ解除動作が確実に禁止される。よって、セキュリティ機器の高いセキュリティレベルを確保することが可能となる。
【００２５】
請求項８に記載の発明によると、セキュリティ制御手段は、管理装置からの機能制限信号をセキュリティ通信手段によって受信すると、ＩＤ登録制御を禁止する。つまり、携帯機に設定されたＩＤコードが記録手段にされなくなるため、携帯機とセキュリティ制御装置との通信が成立しなくなる。このため、該携帯機とセキュリティ制御装置との通信が成立しなくなり、該携帯機を用いたセキュリティ解除動作が確実に禁止される。よって、第三者によるＩＤコードの不正な登録を防止することができ、セキュリティ機器の高いセキュリティレベルを確保することが可能となる。
【００２６】
請求項９に記載の発明によると、管理装置が管理通信手段を備えている場合、制限制御手段は、制限要求信号が入力されると、該管理通信手段を介してセキュリティ制御装置に機能制限信号を送信する。このため、セキュリティ制御装置には該機能制限信号が入力されることとなる。また、管理装置が携帯機用通信手段を備えている場合、制限制御手段は、制限要求信号が入力されると、該携帯機用通信手段を介して携帯機に機能制限信号を送信する。このため、携帯機には該機能制限信号が入力されることとなる。よって、例えば携帯機とセキュリティ制御装置との通信時に、携帯機から機能制限信号をセキュリティ制御装置に送信させるようにすれば、セキュリティ制御装置に該機能制限信号が入力されることとなる。機能制限信号はセキュリティ機器によるセキュリティ解除動作を禁止または制限させるための信号であるため、セキュリティ制御装置は、該機能制限信号が入力されると、セキュリティ解除動作を禁止または制限する。よって、これら何れの場合においても、携帯機の紛失・盗難時には、ユーザが管理装置に制限要求信号を入力することで、該携帯機を用いたセキュリティ解除動作を禁止または制限することができる。それゆえ、セキュリティ機器の高いセキュリティレベルを確保することができる。
【００２７】
請求項１０に記載の発明によると、制限要求信号は、ユーザによって所持される携帯通信機器から送信され、携帯機器用通信手段によって受信される。これにより、該制限要求信号が制限制御手段に入力される。このため、ユーザが携帯機を紛失したり盗難されたりした場合には、携帯通信機器から制限要求信号を送信させることにより、セキュリティ解除動作を禁止または制限することができる。よって、携帯機の紛失・盗難時には、該携帯機によるセキュリティ解除動作を即座に禁止または制限することができ、セキュリティ機器の高いセキュリティレベルを確保することが可能となる。
【発明の効果】
【００２８】
以上詳述したように、本発明によれば、セキュリティ機器のセキュリティレベルをより

一層向上させることができる。

【発明を実施するための最良の形態】

【００２９】

以下、本発明を車両用セキュリティ制御システムに具体化した一実施形態を、図１～図４に基づき詳細に説明する。

図１に示すように、車両用セキュリティ制御システム１は、車両２のユーザ（オーナ）によって所持される携帯機３と、車両２に設けられたセキュリティ制御装置１０と、車両外部の所定箇所に設けられた管理装置３０とを備えている。

【００３０】

携帯機３は通信機能を有し、セキュリティ制御装置１０から送信されるリクエスト信号を受信する受信回路４１と、受信したリクエスト信号が入力されるマイコン（マイクロコンピュータ）４２と、マイコン４２から出力されるＩＤコード信号及び施解錠指令信号を送信する送信回路４３とを備えている。

【００３１】

受信回路４１は、受信したリクエスト信号をパルス信号に復調してマイコン４２に出力する。送信回路４３は、マイコン４２から出力されるＩＤコード信号及び施解錠指令信号を所定周波数の電波に変調して外部に送信する。

【００３２】

マイコン４２は、具体的には図示しないＣＰＵ、ＲＯＭ、ＲＡＭ等からなるＣＰＵユニットであり、不揮発性のメモリ４２ａを備えている。このメモリ４２ａには、携帯機毎に個別に設定されたＩＤコードが予め記録されている。

【００３３】

そして、マイコン４２は、受信回路４１からリクエスト信号が入力されると、メモリ４２ａからＩＤコードを読み込み、該ＩＤコードを含むＩＤコード信号を送信回路４３に送信する。また、マイコン４２には、携帯機３の意匠面に設けられた図示しない操作部が電気的に接続されている。そして、該操作部が操作されると操作信号がマイコン４２に入力され、該マイコン４２は、ＩＤコードと、施錠コードまたは解錠コードとを含む施解錠指令信号を送信回路４３に出力する。

【００３４】

セキュリティ制御装置１０は、携帯機用通信手段としての送信回路１１及び受信回路１２と、セキュリティ制御手段としての車両制御部１３と、セキュリティ通信手段としてのセキュリティ通信部１４とを備えている。そして、車両制御部１３には、送信回路１１、受信回路１２及びセキュリティ通信部１４が電気的に接続されている。

【００３５】

送信回路１１は、車両制御部１３から出力されるリクエスト信号を所定周波数（ここでは１３４ｋＨｚ）の電波に変換し、送信アンテナ１１ａを介して、車両２の周辺の所定領域及び車両２の室内に選択的に該電波を送信する。

【００３６】

受信回路１２は、携帯機３から送信されるＩＤコード信号及び施解錠指令信号を、受信アンテナ１２ａを介して受信し、その受信信号をパルス信号に復調して車両制御部１３へ出力する。

【００３７】

セキュリティ通信部１４は、管理装置３０と通信可能に構成されている。そして、セキュリティ通信部１４は、車両制御部１３から登録信号が入力されると、その登録信号を所定周波数の電波に変調し、該電波を管理装置３０に送信する。また、セキュリティ通信部１４は、管理装置３０から送信される送信信号を受信すると、該送信信号をパルス信号に復調し、該復調した信号を車両制御部１３に出力する。

【００３８】

車両制御部１３は、具体的には図示しないＣＰＵ、ＲＯＭ、ＲＡＭからなるＣＰＵユニットであり、記録手段としての不揮発性のメモリ１３ａを備えている。このメモリ１３ａ

には、携帯機３に設定されたＩＤコードを１つまたは複数個記録可能となっている。

【００３９】

また、車両制御部１３には、モードスイッチ２１と、セキュリティ機器としてのドアロック駆動装置２２及びエンジン制御部２３とが電気的に接続されている。

モードスイッチ２１はユーザによって操作可能なスイッチであり、本実施形態においては車両２の室内に設けられている。そして、このモードスイッチ２１が操作されると、該モードスイッチ２１から車両制御部１３に対して操作信号が出力される。

【００４０】

ドアロック駆動装置２２は、図示しないアクチュエータに接続され、車両制御部１３から駆動信号が入力されると、該アクチュエータを駆動してドア錠を自動的に施解錠する。また、ドアロック駆動装置２２は、ドア錠の施解錠状態を示す施解錠状態信号を車両制御部１３に出力する。このため、車両制御部１３は、該施解錠状態信号に基づき、ドア錠の施解錠状態を認識可能となる。

【００４１】

エンジン制御部２３は、図示しないセルモータに接続され、車両制御部１３から始動信号が入力されると、同セルモータを駆動するとともに、燃料噴射制御や点火制御を行って、エンジンを自動的に始動させる。また、エンジン制御部２３は、エンジンの駆動状態を示す駆動状態信号を車両制御部１３に出力する。このため、車両制御部１３は、該駆動状態信号に基づき、エンジンの駆動状態を認識可能となる。

【００４２】

車両制御部１３は、車両登録モードと、ＩＤ登録モードと、セキュリティ制御モードとを有している。ここで、車両登録モードとは、車両２を管理装置３０の管理対象として登録する車両登録制御を行うモードを示す。また、ＩＤ登録モードとは、携帯機３に設定されたＩＤコードをメモリ１３ａに記録（登録）するＩＤ登録制御を行うモードを示す。また、セキュリティ制御モードとは、ＩＤ登録された携帯機３との通信に基づいてドアロック駆動装置２２やエンジン制御部２３を制御するモードを示す。そして、車両制御部１３は、モードスイッチ２１から操作信号が入力された際にＩＤ登録モードまたは車両登録モードとなり、それ以外はセキュリティ制御モードとなる。すなわち、車両制御部１３は、通常、セキュリティ制御モードとなっており、モードスイッチ２１が操作されることにより、ＩＤ登録モードや車両登録モードに切り換わるようになっている。なお、ここではモードスイッチ２１の操作によりＩＤ登録モードまたは車両登録モードに切り換わるようになっているが、これに限らず、モードスイッチ２１の操作によりＩＤ登録モードに切り換わり、他のスイッチなどの操作により車両登録モードに切り換わるようになっていてもよい。つまり、個別の操作によってＩＤ登録モードまたは車両登録モードに切り換わるようになっていてもよい。

【００４３】

こうした車両制御部１３は、車両登録モードに切り換わると車両登録制御を行う。

詳しくは、車両制御部１３には、図示しない入力装置（例えばカーナビゲーションシステムなどの入力部）からの入力信号が入力可能となっている。そして、車両登録モードに切り換わった後、ユーザによって設定可能な機能制限用暗証番号が該入力装置に入力され、該機能制限用暗証番号からなる入力信号が車両制御部１３に入力されると、車両制御部１３は、車両情報と機能制限用暗証コードとを含む車両登録信号を、セキュリティ通信部１４を介して管理装置３０に送信する。なお、車両情報とは車両２を特定するための情報であり、本実施形態において車両情報には、車両２の車体番号、車両番号、ディーラー情報（ディーラーに固有に設定された店舗番号やパスワード等）のうちの少なくとも１つが含まれている。機能制限用暗証コードとは、機能制限用暗証番号をバイナリー変換したものに相当する。

【００４４】

また、管理装置３０から送信される車両登録完了信号がセキュリティ通信部１４を介して車両制御部１３に入力されると、該車両制御部１３は、車両２の室内に設けられた図示

しないインジケータに、車両２の登録が完了した旨を示す表示を行う。

【００４５】

これに対し、ＩＤ登録モードに切り換わると、車両制御部１３は登録通信制御を行う。

詳しくは、車両制御部１３は、送信回路１１に対してリクエスト信号を間欠的に出力し、送信回路１１及び送信アンテナ１１ａを介して、車両２の室内にリクエスト信号を送信する。そして、該リクエスト信号に応答して送信された携帯機３からのＩＤコード信号を受信回路１２及び受信アンテナ１２ａによって受信し、該受信回路１２からＩＤコード信号が入力されると、車両制御部１３は、該ＩＤコード信号に含まれるＩＤコードをメモリ１３ａに記録する。そして、車両制御部１３は、該ＩＤコードの記録を完了すると、セキュリティ通信部１４に対して該ＩＤコードと車両情報とを含む登録信号を出力し、該セキュリティ通信部１４を介して登録信号を管理装置３０に送信する。

【００４６】

一方、セキュリティ制御モードにおいて車両制御部１３は、送信回路１１に対してリクエスト信号を間欠的に出力する。このため、送信回路１１及び送信アンテナ１１ａを介して、車両２の周辺の所定領域及び車両２の室内に選択的にリクエスト信号が送信される。また、車両制御部１３は、受信回路１２から前記ＩＤコード信号または施解錠指令信号が入力されると、それらの信号に含まれるＩＤコードと、メモリ１３ａに記録されているＩＤコードとの比較（ＩＤコード照合）を行う。そして、車両制御部１３は、それらＩＤコード同士が一致したこと、すなわちＩＤコード照合が成立したことを条件として、ドアロック駆動装置２２やエンジン制御部２３の駆動制御を行う。

【００４７】

詳しくは、ＩＤコード信号が入力された場合、車両制御部１３は、該ＩＤコード信号が、車両２の周辺の所定領域に送信されたリクエスト信号に応答したものであれば、ドアロック駆動装置２２に駆動信号を出力してドア錠を解錠させる。そして、車両制御部１３は、該ＩＤコード信号が入力されなくなると、ドアロック駆動装置２２に駆動信号を出力してドア錠を施錠させる。

【００４８】

これに対し、車両制御部１３は、入力されたＩＤコード信号が、車両２の室内に送信されたリクエスト信号に応答したものであれば、エンジン始動待機状態となる。そして、車両制御部１３は、このエンジン始動待機状態において図示しないスタートスイッチから操作信号が入力されると、エンジン制御部２３に対して始動信号を出力してエンジンを始動させる。つまり、車両制御部１３は、エンジン始動待機状態でない場合には、たとえスタートスイッチから操作信号が入力されてもエンジン制御部２３に始動信号を出力しない。なお、スタートスイッチは、車両２の室内において運転席の近辺に設けられたスイッチであり、車両制御部１３と電気的に接続されている。

【００４９】

また、施解錠指令信号が入力された場合、車両制御部１３は、該施解錠指令信号に施錠コードが含まれていればドア錠を施錠させ、解錠コードが含まれていればドア錠を解錠させる。

【００５０】

このように、セキュリティ制御モードにおいてセキュリティ制御装置１０は、携帯機３との通信を行い、該携帯機３との通信の成立有無に基づいてドアロック駆動装置２２やエンジン制御部２３といったセキュリティ機器を制御する。

【００５１】

管理装置３０は専用の管理センターなどに配設されており、管理通信手段としての管理通信部３１と、制限制御手段としての管理制御部３２と、携帯機器用通信手段及び受信手段としての携帯機器用通信部３３とを備えている。そして、管理制御部３２には、管理通信部３１及び携帯機器用通信部３３が電気的に接続されている。

【００５２】

管理通信部３１は、セキュリティ制御装置１０のセキュリティ通信部１４と通信可能と

なっており、該セキュリティ通信部１４から送信される車両登録信号や登録信号を受信すると、それら信号を復調して管理制御部３２に出力する。

【００５３】

携帯機器用通信部３３は、ユーザによって所持される携帯通信機器（ここでは携帯電話４）と通信可能となっている。

携帯電話４は、前記機能制限用暗証番号が例えばテンキーから入力された際に制限操作が行われたと判断し、該機能制限用暗証番号をバイナリー変換した機能制限用暗証コードを含む制限要求信号を、管理装置３０に送信する。また、機能制限用暗証番号とともに携帯機３を指定する携帯機指定番号がテンキーから入力された場合には、携帯電話４は、機能制限用暗証コードと携帯機指定コードとを含む制限要求信号を、管理装置３０に送信する。ここで、携帯機指定番号とは、前記管理装置３０のメモリ３２ａに記録されたＩＤコードの登録番号を示すものであり、携帯機指定コードとは、該携帯機指定番号をバイナリー変換したものに相当する。

【００５４】

そして、携帯機器用通信部３３は、携帯電話４から送信される制限要求信号を受信すると、該制限要求信号を復調して管理制御部３２に出力する。また、携帯機器用通信部３３は、管理制御部３２から制限完了信号が入力されると、その制限完了信号を、公衆通信回線などを用いて携帯電話４に送信する。なお、携帯電話４は、携帯機器用通信部３３から送信される制限完了信号を受信すると、音、振動、表示などにより、その旨をユーザに通知するようになっている。

【００５５】

管理制御部３２は、具体的には図示しないＣＰＵ、ＲＯＭ、ＲＡＭからなるＣＰＵユニットであり、不揮発性のメモリ３２ａを備えている。

このメモリ３２ａには、管理対象として設定された車両２の車両情報が記録されている。詳しくは、メモリ３２ａには、車両情報として、車両２の車体番号、車両番号、ディーラー情報（ディーラーに固有に設定された店舗番号やパスワード等）、前記携帯電話４の機器情報（電話番号、メールアドレス等）など、車両２を特定するための情報が記録されている。

【００５６】

また、メモリ３２ａには、前記車両登録制御時にセキュリティ制御装置１０から送信される機能制限用暗証コード、及び前記登録通信制御時にセキュリティ制御装置１０から送信されるＩＤコードが、それぞれ車両情報に対応付けされた状態で記録可能となっている。詳しくは、メモリ３２ａには、該車両情報に対応して、機能制限用暗証コードの記録領域及びＩＤコードの記録領域（ＩＤ記録領域）が設定されている。例えば、メモリ３２ａに２台の車両２の車両情報Ａ，Ｂが記録されている場合、車両情報Ａに対応する機能制限用暗証コードの記録領域及びＩＤ記録領域と、車両情報Ｂに対応する機能制限用暗証コードの記録領域及びＩＤ記録領域とが個別に設定されている。なお、該ＩＤ記録領域には、複数のＩＤコードを記録可能となっており、その記録可能なＩＤコードの数は、予め設定された規定数またはユーザによって設定された規定数となっている。また、該記録領域に記録されるＩＤコードには、例えば記録された順番などからなる登録番号が対応付けされている。

【００５７】

管理制御部３２は、管理通信部３１から車両登録信号が入力されると、該車両登録信号に含まれる車両情報及び機能制限用暗証コードを、対応付けした状態でメモリ３２ａに記録する。そして、管理制御部３２は、車両登録が完了した旨を示す車両登録完了信号を、管理通信部３１を介してセキュリティ制御装置１０に送信する。

【００５８】

また、管理制御部３２は、管理通信部３１から登録信号が入力されると、該登録信号に含まれる車両情報と対応するＩＤ記録領域に、同登録信号に含まれるＩＤコードを記録する。そして、管理制御部３２は、該記録が完了した旨を示す登録完了信号を、管理通信部

３１を介してセキュリティ制御装置１０に送信する。

【００５９】

さらに、管理制御部３２は、携帯機器用通信部３３から制限要求信号が入力されると、メモリ３２ａに既に記録されている機能制限用暗証コードから、該制限要求信号に含まれる機能制限用暗証コードと対応する機能制限用暗証コードの有無を判断する（暗証コード有無判断）。その結果、制限要求信号に含まれる機能制限用暗証コードと対応する機能制限用暗証コードがメモリ３２ａに存在する場合、管理制御部３２は、該機能制限用暗証コードと対応する車両情報に基づき、制限指令制御の管理対象となる車両２を特定する。そして、管理制御部３２は、その特定した車両２に搭載されたセキュリティ制御装置１０に、機能制限コードを含む機能制限信号を、管理通信部３１を介して送信する。また、制限要求信号に前記携帯機指定コードが含まれている場合、管理制御部３２は、メモリ３２ａに車両情報と対応して記録されたＩＤコードのうち、携帯機指定コードと一致する登録番号が対応付けされたＩＤコードを読み出す。そして、管理制御部３２は、読み出したＩＤコードと前記機能制限コードとを含む機能制限信号を、管理通信部３１を介して送信する。また、管理制御部３２は、管理通信部３１から制限完了信号が入力されると、該制限完了信号を、携帯機器用通信部３３を介して携帯電話４に送信する。

【００６０】

一方、セキュリティ制御装置１０は、管理装置３０から送信される機能制限信号を受信すると、前述した携帯機３との通信に基づくドアロック駆動装置２２やエンジン制御部２３の駆動を制限または禁止する機能制限処理を行う。

【００６１】

詳しくは、まず、セキュリティ制御装置１０は、機能制限信号をセキュリティ通信部１４によって受信する。このため、該機能制限信号は、車両制御部１３に入力される。車両制御部１３は、機能制限信号が入力されると、機能制限処理を行う状態になったことを示す制限完了信号を、セキュリティ通信部１４を介して管理装置３０に送信する。また、車両制御部１３は、該機能制限信号にＩＤコードが含まれているか否かを判断する。その結果、機能制限信号にＩＤコードが含まれていない場合、車両制御部１３は、通信可能となっている何れの携帯機３との通信が成立しても、ドアロック駆動装置２２やエンジン制御部２３の制御を制限または禁止する。すなわち、この場合、車両制御部１３は、メモリ１３ａに記録されている全てのＩＤコードと対応する携帯機３との通信が成立しても、セキュリティ機器（ドアロック駆動装置２２やエンジン制御部２３）のセキュリティ解除を制限または禁止する。また、機能制限信号にＩＤコードが含まれている場合、車両制御部１３は、該ＩＤコードと対応する携帯機３との通信が成立した場合にのみ、ドアロック駆動装置２２やエンジン制御部２３の制御を制限または禁止する。

【００６２】

なお、本実施形態において車両制御部１３は、以下の＜ａ＞または＜ｂ＞に示す機能制限処理を行うようになっており、これらのうちのどちらの処理を行うかについては、ユーザによって設定可能となっている。

【００６３】

＜ａ＞第１機能制限処理（セキュリティ解除禁止処理）

（ａ－１）機能制限信号にＩＤコードが含まれていない場合

この場合、車両制御部１３は、リクエスト信号に応答して送信された携帯機３からのＩＤコード信号や携帯機３からの施解錠指令信号を受信すると、それらＩＤコード信号や施解錠指令信号に含まれるＩＤコードがメモリ１３ａに記録されていたとしても、ドアロック駆動装置２２やエンジン制御部２３の制御を行わない。すなわち、車両制御部１３は、携帯機３との通信が成立しても、ドア錠の解錠やエンジンの始動を禁止する。換言すれば、機能制限信号が入力されると車両制御部１３は、ドアロック駆動装置２２によるドア錠の解錠やエンジン制御部２３によるエンジンの始動許可といったセキュリティ解除動作を禁止する。

【００６４】

（ａ－２）機能制限信号にＩＤコードが含まれている場合

この場合、車両制御部１３は、リクエスト信号に応答して送信された携帯機３からのＩＤコード信号や携帯機３からの施解錠指令信号を受信すると、まず、該ＩＤコード信号や施解錠指令信号に含まれるＩＤコードと機能制限信号に含まれるＩＤコードとを比較する。その結果、車両制御部１３は、それらＩＤコード同士が一致した場合に限り、ドアロック駆動装置２２やエンジン制御部２３の制御を行わない。すなわち、この場合、車両制御部１３は、機能制限信号に含まれるＩＤコードと対応する携帯機３との通信が成立した場合にのみ、ドア錠の解錠やエンジンの始動、すなわちセキュリティ解除動作を禁止する。よって、車両制御部１３は、メモリ１３ａに記録された他のＩＤコード（機能制限信号に含まれていないＩＤコード）を含むＩＤコード信号や施解錠指令信号を受信した場合には、セキュリティ解除動作を通常どおり行う。つまり、ここでは、特定の携帯機３を用いたセキュリティ解除動作のみが禁止される。

【００６５】

＜ｂ＞第２機能制限処理（セキュリティ解除制限処理）

（ｂ－１）機能制限信号にＩＤコードが含まれていない場合

この場合、車両制御部１３は、車両２の室外に送信したリクエスト信号に応答して送信された携帯機３からのＩＤコード信号や携帯機３からの施解錠指令信号を受信すると、ドアロック駆動装置２２を駆動制御してドア錠の施解錠制御を行う。しかし、車両２の室内に送信したリクエスト信号に応答して送信された携帯機３からのＩＤコード信号を受信した場合においては、車両制御部１３は、エンジン始動許可状態にはならない。このため、たとえスタートスイッチが操作されても、車両制御部１３はエンジン制御部２３の制御を行わない。すなわち、車両制御部１３は、携帯機３との通信が成立した場合、ドア錠の施解錠を行うものの、エンジンの始動については禁止する。換言すれば、機能制限信号が入力されると車両制御部１３は、セキュリティ解除動作を制限する。

【００６６】

（ｂ－２）機能制限信号にＩＤコードが含まれている場合

この場合においても、車両制御部１３は、車両２の室外に送信したリクエスト信号に応答して送信された携帯機３からのＩＤコード信号や携帯機３からの施解錠指令信号を受信すると、ドアロック駆動装置２２を駆動制御してドア錠の施解錠制御を行う。つまり、ここでは、車両制御部１３は、機能制限信号にＩＤコードが含まれていないときと同様にドア錠の施解錠制御を行う。しかし、ＩＤコードを含む機能制限信号が入力された後に、車両２の室内に送信したリクエスト信号に応答して送信された携帯機３からのＩＤコード信号を受信した場合には、車両制御部１３は、まず該ＩＤコード信号に含まれるＩＤコードが機能制限信号に含まれるＩＤコードとを比較する。その結果、ＩＤコード信号に含まれるＩＤコードが機能制限信号に含まれるＩＤコードと一致した場合に限り、車両制御部１３は、エンジン始動許可状態にはならない。すなわち、この場合、車両制御部１３は、機能制限信号に含まれるＩＤコードと対応する携帯機３との通信が成立した場合には、ドア錠の施解錠を行うものの、エンジンの始動については禁止する。換言すれば、ＩＤコードを含む機能制限信号が入力されると、車両制御部１３は、該ＩＤコードと対応する携帯機３との通信に基づくセキュリティ解除動作のみを制限する。よって、車両制御部１３は、メモリ１３ａに記録された他のＩＤコード（機能制限信号に含まれていないＩＤコード）を含むＩＤコード信号や施解錠指令信号を受信した場合には、セキュリティ解除動作を通常どおり行う。つまり、ここでは、特定の携帯機３を用いたセキュリティ解除動作のみが制限される。

【００６７】

なお、車両制御部１３は、制限制御を解除する旨を示す制限解除信号が入力された際に、こうした機能制限制御を解除して通常のセキュリティ制御モードに切り換わる。このため、例えば制限解除信号となる制限解除番号を携帯電話４に入力し、携帯電話４、管理装置３０及びセキュリティ制御装置１０間の通信を行わせ、該制限解除信号をセキュリティ制御装置１０に受信させれば、通常のセキュリティ制御モードに切り換わる。

【００６８】
次に、本実施形態の車両用セキュリティ制御システム１において、車両２の車両情報を管理装置３０に登録して車両２を管理装置３０の管理対象として設定する車両登録制御時における通信態様を、図２に示すシーケンスチャートを用いて説明する。
【００６９】
同図に示すように、管理装置３０への車両２の登録は、セキュリティ制御装置１０と管理装置３０との間の通信によって行われる。
詳しくは、まず、セキュリティ制御装置１０は、モードスイッチ２１により車両登録モードへの移行操作が行われると、車両登録モードに切り換わる（ステップＳ１）。ここで、前記入力装置から機能制限用暗証番号が入力されると（ステップＳ２）、セキュリティ制御装置１０は、車両２の車両情報と機能制限用暗証コードとを含む車両登録信号を、管理装置３０に送信する（ステップＳ３）。
【００７０】
管理装置３０は、セキュリティ制御装置１０からの車両登録信号を受信すると、該車両登録信号に含まれる車両情報及び機能制限用暗証コードをメモリ３２ａに記録し、管理対象となる車両２の登録（管理車両登録）を完了する（ステップＳ４）。このため、セキュリティ制御装置１０（車両２）は、管理対象として管理装置３０に登録される。そして、管理装置３０は、車両登録が完了した旨を示す車両登録完了信号を、セキュリティ制御装置１０に送信する（ステップＳ５）。
【００７１】
セキュリティ制御装置１０は、管理装置３０からの車両登録完了信号を受信すると、車両２の登録が完了した旨を車両室内のインジケータに表示することにより、登録完了の旨を通知する（ステップＳ６）。このため、ユーザは、該インジケータを視認することにより、車両２の登録が完了したことを確実に認識可能となる。
【００７２】
次に、本実施形態の車両用セキュリティ制御システム１において、携帯機３のＩＤコードをセキュリティ制御装置１０に登録するＩＤ登録制御時における通信態様を、図３に示すシーケンスチャートを用いて説明する。
【００７３】
同図に示すように、ＩＤ登録制御時には、携帯機３と、セキュリティ制御装置１０と、管理装置３０との間の通信によって行われる。
まず、セキュリティ制御装置１０のモードスイッチ２１がユーザによって操作されると（ステップＳ１１）、セキュリティ制御装置１０はセキュリティ制御モードからＩＤ登録モードに切り換わる（ステップＳ１２）。ＩＤ登録モードに切り換わるとセキュリティ制御装置１０は、車両２の室内に前記リクエスト信号を送信する（ステップＳ１３）。
【００７４】
そして、携帯機３は、このリクエスト信号を受信すると、前記ＩＤコード信号を送信する（ステップＳ１４）。
セキュリティ制御装置１０は、携帯機３からのＩＤコード信号を受信すると、該ＩＤコード信号に含まれるＩＤコードをメモリ１３ａに記録する（ステップＳ１５）。すなわち、セキュリティ制御装置１０は、取得した携帯機３のＩＤコードを自身に登録する。次いで、セキュリティ制御装置１０は、管理装置３０に前記登録信号を送信する（ステップＳ１６）。
【００７５】
管理装置３０は、セキュリティ制御装置１０からの登録信号を受信すると、該登録信号に含まれるＩＤコードを、メモリ３２ａにおいて車両情報と対応するＩＤ記録領域に記録する（ステップＳ１７）。また、管理装置３０は、前記登録完了信号をセキュリティ制御装置１０に送信する（ステップＳ１８）。このため、管理装置３０は、記録したＩＤコードに基づき、車両２に対応する携帯機３の管理が可能となる。
【００７６】

セキュリティ制御装置１０は、管理装置３０からの登録完了信号を受信すると、車両２の室内に設けられた図示しないインジケータに登録完了の旨を示す表示を行ったり、図示しないスピーカなどから該登録完了の旨を示す音響報知を行ったりする（ステップＳ１９）。このため、ユーザは、携帯機３の登録が完了したことを確実に認識可能となる。

【００７７】

次に、本実施形態の車両用セキュリティ制御システム１において、セキュリティ解除動作を禁止または制限する機能制限制御時における通信態様を、図４に示すシーケンスチャートを用いて説明する。

【００７８】

同図に示すように、機能制限制御は、セキュリティ制御装置１０と、管理装置３０と、携帯電話４との間の通信によって行われる。

詳しくは、まず、携帯電話４は、前記制限操作が行われて機能制限用暗証番号が入力されると（ステップＳ２１）、機能制限用暗証コードを含む前記制限要求信号を管理装置３０に送信する（ステップＳ２２）。ここで、携帯電話４は、機能制限用暗証番号とともに携帯機指定番号が入力された場合には、機能制限用暗証コードと携帯機指定コードとを含む制限要求信号を管理装置３０に送信する。

【００７９】

管理装置３０は、制限要求信号が入力されると、該制限要求信号に含まれる機能制限用暗証コードに基づいて、対応する車両２を特定する（ステップＳ２３）。そして、管理装置３０は、特定した車両２に設けられたセキュリティ制御装置１０に対して、機能制限コードを含む前記機能制限信号を送信する（ステップＳ２４）。ここで、管理装置３０は、携帯機指定コードを含む制限要求信号が入力された場合には、該携帯機指定コードと対応するＩＤコード及び機能制限コードを含む機能制限信号を送信する。

【００８０】

セキュリティ制御装置１０は、管理装置３０から機能制限信号が入力されると、制限完了信号を管理装置３０に送信する（ステップＳ２５）。また、セキュリティ制御装置１０は、前記＜ａ＞または＜ｂ＞に示した機能制限処理を行う（ステップＳ２６）。

【００８１】

管理装置３０は、制限完了信号を受信すると、その制限完了信号を携帯電話４に送信する（ステップＳ２７）。つまり、管理装置３０は、セキュリティ制御装置１０から送信された制限完了信号を携帯電話４に送信するための通信中継手段として機能する。

【００８２】

そして、携帯電話４は、制限完了信号を受信すると、セキュリティ制御装置１０が機能制限状態にある旨を、音、振動、表示などによってユーザに報知する。

したがって、本実施形態によれば以下のような効果を得ることができる。

【００８３】

（１）ユーザによって所持される携帯通信機器（携帯電話４）から送信される制限要求信号が管理装置３０によって受信されると、管理装置３０からセキュリティ制御装置１０に対して機能制限信号が送信される。セキュリティ制御装置１０は、機能制限信号を受信したことを条件として、ドアロック駆動装置２２やエンジン制御部２３の制御を禁止または制限する。すなわち、セキュリティ制御装置１０は、該機能制限信号の受信を条件として、セキュリティ機器によるセキュリティ解除動作を禁止または制限する。このため、ユーザが携帯機３を紛失したり盗難されたりした場合には、携帯電話４から制限要求信号を送信させることにより、セキュリティ制御装置１０によるセキュリティ解除動作を禁止または制限することができる。よって、携帯機３の紛失・盗難時においても、該携帯機３によるセキュリティ解除動作を即座に禁止または制限することができ、セキュリティ機器の高いセキュリティレベルを確保することができる。

【００８４】

（２）第三者が携帯機３を盗難しても、該携帯機３を用いたセキュリティ解除動作がユーザによって簡単に禁止または制限されてしまうため、盗難後の携帯機３の価値は実質的

に低下する。よって、第三者は、携帯機３を盗難しようとする気すら沸かなくなる。つまり、第三者による携帯機３の盗難の意欲自体を減退させることができ、携帯機３の盗難防止性も向上する。

【００８５】

（３）携帯電話４で制限操作を行う際に、携帯機３を指定する携帯機指定番号がユーザによって入力されると、セキュリティ制御装置１０は、該指定された携帯機３との通信に基づくセキュリティ解除のみを禁止または制限する。すなわち、携帯電話４で制限操作を行う際に、制限すべき携帯機３の指定を行えば、特定の携帯機３によるセキュリティ解除のみを禁止または制限させることができる。このため、例えば携帯機３を紛失したり盗難されたりした場合、その携帯機３によるセキュリティ解除のみを禁止または制限することができ、他に登録されている携帯機３によるセキュリティ解除については通常どおり可能となる。つまり、紛失したり盗難されたりしていない携帯機３については、何ら制限を受けることなく利用可能となる。よって、機能制限が不要な携帯機３によるセキュリティ解除までをも禁止または制限してしまうことがなく、携帯機３の利便性を確保することができる。

【００８６】

なお、本発明の実施形態は以下のように変更してもよい。

・　セキュリティ制御装置１０は、第１機能制限処理（セキュリティ解除禁止処理）に設定されている状態おいてＩＤコードを含んでいない機能制限信号を受信した場合（前記（ａ－１）の場合）には、携帯機３との通信自体を禁止するようになっていてもよい。このように変更すれば、機能制限信号が車両制御部１３に入力されると、セキュリティ制御モードにおけるセキュリティ制御装置１０と携帯機３との通信が不能となる。よって、携帯機３と車両制御部１３との通信が成立しなくなり、車両制御部１３によるドアロック駆動装置２２及びエンジン制御部２３の制御が確実に禁止される。したがって、セキュリティ機器の高いセキュリティレベルを確保することができる。しかも、この場合、セキュリティ制御装置１０は、機能制限信号を受信すると、セキュリティ制御モード時においてリクエスト信号を送信しなくなる。また、携帯機３は、リクエスト信号を受信しないため、ＩＤコード信号を送信しなくなる。よって、携帯機３とセキュリティ制御装置１０との間での無駄な通信を防止することができ、携帯機３及びセキュリティ制御装置１０の電力消費量を低減させることができる。

【００８７】

・　前記実施形態において管理装置３０は、セキュリティ制御装置１０に対して機能制限信号を送信するようになっている。しかし、例えば図１に２点鎖線で示すように、管理装置３０と通信可能な携帯機側通信部４４を携帯機３に設け、該機能制限信号を、管理装置３０から携帯機３に対して送信させるようにしてもよい。そしてこの場合、携帯機３が該機能制限信号を受信した後におけるセキュリティ制御装置１０との通信時には、機能制限コードを含む送信信号（ＩＤコード信号、施解錠指令信号）を携帯機３から送信させるように変更する。一方、セキュリティ制御装置１０が該機能制限コードを含む送信信号を受信した際には、セキュリティ制御動作を禁止または制限する制御を行うようにセキュリティ制御装置１０を変更する。このようにしても、携帯機３の紛失・盗難時には、該携帯機３を用いたセキュリティ解除動作が確実に禁止または制限される。よって、セキュリティ機器の高いセキュリティレベルを確保することができる。

【００８８】

また、機能制限信号を受信した携帯機３は、ＩＤコード信号、施解錠指令信号を送信不能となっていてもよい。

・　セキュリティ制御装置１０は、機能制限信号を受信した際には、携帯機３との通信に基づくセキュリティ解除動作を禁止または制限を行うことに加えて、ＩＤ登録モードに切り換わらないようになるなどして前記ＩＤ登録制御を禁止するようになっていてもよい。このようにすれば、新たに登録を試みた携帯機３を用いたセキュリティ解除動作が確実に禁止される。よって、第三者によるＩＤコードの不正な登録を防止することができ、セ

キュリティ機器の高いセキュリティレベルを確保することが可能となる。

【００８９】

・ 前記実施形態では、セキュリティ制御装置１０は、機能制限状態になると、その旨を示す制限完了信号を、管理装置３０を介して携帯電話４に送信するようになっている。しかし、セキュリティ制御装置１０から携帯電話４に対して、管理装置３０を介することなく、電話回線等によって直接的に制限完了信号を送信するようになっていてもよい。

【００９０】

・ 前記実施形態では、セキュリティ制御装置１０から管理装置３０を介して携帯電話４に制限完了信号が送信されることにより、セキュリティ制御装置１０が機能制限状態になった旨が携帯電話４に通知されるようになっている。しかし、管理装置３０がセキュリティ制御装置１０に機能制限信号を送信した際に、該管理装置３０から制限完了信号を携帯電話４に送信するように変更してもよい。つまりこの場合、管理装置３０は、セキュリティ制御装置１０に機能制限信号を送信したことをもって、該セキュリティ制御装置１０が機能制限状態になったと判断して、その旨を携帯電話４に通知するようになっていてもよい。

【００９１】

・ 前記実施形態において、セキュリティ制御装置１０の車両制御部１３とセキュリティ通信部１４との間で、互いが正常に動作しているか否かを判断するための相互認証（ペアリング）を行わせてもよい。そして、互いが正常に動作していると判断された場合、すなわち該相互認証が成立した場合にのみ、携帯機３のＩＤコードをセキュリティ制御装置１０に登録可能としてもよい。このようにすれば、例えばセキュリティ通信部１４が不正に取り外されたり破壊されたりした場合には両者間での相互認証が成立しなくなるため、セキュリティ制御装置１０に登録できない。よって、ＩＤコードの不正な登録をより確実に防止できる。

【００９２】

・ 携帯機３にＧＰＳモジュールを設け、機能制限時には携帯機３の位置を管理装置３０によって認識し、該携帯機３の位置を管理装置３０から携帯電話４に通知するようにしてもよい。このようにすれば、紛失したり盗難されたりした携帯機３の所在をユーザは確実に認識することができる。

【００９３】

・ 前記実施形態では、携帯電話４から管理装置３０に対して制限要求信号が送信されるようになっている。しかし、車両２にてユーザによる制限操作を可能とし、セキュリティ制御装置１０から管理装置３０に対して制限要求信号を送信可能としてもよい。すなわち、車両２にて制限操作を行うことにより、セキュリティ機器（ドアロック駆動装置２２やエンジン制御部２３）の機能制限を可能としてもよい。このようにすれば、機能制限を行う際に、携帯電話４などの携帯通信機器が不要となる。

【００９４】

・ 前記各実施形態では、車両２を管理装置３０の管理対象として設定するための車両登録制御時に、セキュリティ制御装置１０から管理装置３０に車両登録信号を送信させるようになっている。しかし、こうした車両登録制御時においては、セキュリティ制御装置１０とは別に設けられた登録装置から管理装置３０に前記車両登録信号を送信可能としてもよい。例えば登録装置としてパーソナルコンピュータを用い、該パーソナルコンピュータから管理装置３０に車両登録信号を送信可能としてもよい。この場合、車両情報や機能制限用暗証番号などの車両登録情報をパーソナルコンピュータに入力し、インターネットなどの通信網を介して、該車両登録情報を含む車両登録信号を管理装置３０に送信させるようにする。このようにすれば、車両登録作業に必ずしもセキュリティ制御装置１０（車両２）が必要ではなくなるため、該車両登録作業の利便性が向上する。また、ユーザ、ディーラー、携帯機３のメーカーなどによって設定されたパスワードを車両登録信号に付与すれば、第三者による不正な車両登録を防止することができる。

【００９５】

なお、車両２を管理装置３０に登録する作業（車両登録作業）や、携帯機３のＩＤコードをセキュリティ制御装置１０に登録する作業（ＩＤ登録作業）は、ユーザに限らず、ディーラーや携帯機３のメーカーなど、ユーザにとって信頼できる作業者によって行われるようになっていてもよい。

【００９６】

・　前記実施形態において、セキュリティ制御装置１０と管理装置３０との間の通信は、無線通信に限らず、例えば公衆通信回線を用いた有線通信が採用されてもよい。例えば、電話のモジュラージャックが接続される接続口を車両２に設け、セキュリティ制御装置１０と管理装置３０との通信を、電話線を用いて行うようにしてもよい。

【００９７】

・　前記各実施形態において、携帯通信機器は、携帯電話４に限らず、例えば、ノート型のパーソナルコンピュータや、ＰＤＡ（Personal Digital Assistance ：携帯情報端末）や、専用の通信機器などであってもよい。

【００９８】

・　前記各実施形態の車両用セキュリティ制御システム１は、携帯機３とセキュリティ制御装置１０との相互通信により、携帯機３が車両２に近づくことでドア錠が自動的に解錠される機能（スマートエントリ機能）と、携帯機３が車両２の室内に進入することでエンジンの始動が許可される機能（スマートイグニッション機能）とを備えている。しかし、車両用セキュリティ制御システム１は、こうしたスマートエントリ機能やスマートイグニッション機能を備えていなくてもよい。例えば、携帯機３は、トランスポンダと機械鍵とを備え、該機械鍵を車両２に装着した際に、セキュリティ制御装置１０との相互通信を行うようになっていてもよい。そして、セキュリティ制御装置１０は、該トランスポンダとの相互通信が成立した際に機械鍵の回動操作を許可するとともに、該機械鍵が回動操作されたことを条件として、ドアロック駆動装置２２やエンジン制御部２３を制御するようになっていてもよい。つまり、セキュリティ制御装置１０は、携帯機３との相互通信に基づいてセキュリティ解除動作を行うようになっていればよい。

【００９９】

また、こうした携帯機３とセキュリティ制御装置１０との相互通信についても必須でなくてもよい。例えば、携帯機３は、前記施解錠指令信号のみを送信可能となっていてもよく、それとともに、セキュリティ制御装置１０は、送信回路１１を備えず、リクエスト信号を送信しないように構成されていてもよい。つまり、セキュリティ制御装置１０は、携帯機３との通信に基づいてセキュリティ解除動作を行うようになってさえいれば、必ずしも携帯機３との相互通信を行うようになっている必要はない。

【０１００】

・　前記実施形態において、管理装置３０は、管理対象となる車両２に設けられたセキュリティ制御装置１０に登録可能な携帯機３のＩＤコードの数を管理するようになっている。しかし、管理装置３０は、必ずしも該ＩＤコードの数を管理するようになっている必要はない。

【０１０１】

また、管理装置３０は、必ずしも携帯機３のＩＤコードを管理しなくてもよい。つまり、管理装置３０は、必ずしもメモリ３２ａにＩＤコードを記録するようになっていなくてもよい。このようにすれば、管理装置３０のメモリ３２ａの記録負担を軽減することができるとともに、セキュリティ制御装置１０と管理装置３０との間で、登録信号や登録完了信号の送受信を行う必要がなくなり、両者の通信負担を軽減することができる。但しこの場合、所定の携帯機３によるセキュリティ解除動作のみを禁止または制限させる制御（前記（ａ－２）及び（ｂ－２）に示される制御）をセキュリティ制御装置１０に行わせることはできなくなる。

【０１０２】

そこで、こうした変更例にあっては、管理装置３０は、例えば携帯機指定コードを含む制限要求信号を受信した際に、その携帯機指定コードを含む機能制限信号をセキュリティ

制御装置１０に送信するように変更されてもよい。そして、セキュリティ制御装置１０のメモリ１３ａに記録されるＩＤコードに、携帯機指定コードと対応する登録番号を付与してもよい。このようにすれば、セキュリティ制御装置１０は、機能制限信号に含まれる携帯機指定コードとメモリ１３ａに記録された登録番号とに基づいて、所定の携帯機３との通信によるセキュリティ解除動作のみを禁止または制限することができる。

【０１０３】

・　前記各実施形態において車両用セキュリティ制御システム１は、セキュリティ制御装置１０さえＩＤ登録モードに切り換えれば、どこでも携帯機３の登録が可能となっている。しかし、例えばセキュリティ制御装置１０にＧＰＳモジュールを接続するなどして、セキュリティ制御装置１０が予め設定された所定の場所（例えば自宅、会社、ディーラーなど）でのみ、携帯機３の登録が可能となるように車両用セキュリティ制御システム１を変更してもよい。このようにすれば、第三者によるＩＤコードの不正な登録をさらに防止することができ、セキュリティ機器のセキュリティレベルをさらに向上させることができる。なお、こうした変更は、携帯機３の登録場所に限らず、車両２を管理装置３０の管理対象として登録する車両登録が可能な場所についても同様に限定してもよい。

【０１０４】

・　前記実施形態において、セキュリティ制御装置１０をＩＤ登録モードに切り換えるための操作は、モードスイッチ２１の操作に限定されない。例えば、セキュリティ制御装置１０は、車両２に設けられた既存のスイッチ（例えばレバーコンビネーションスイッチなど）を、所定の態様（ユーザやディーラーによるプリセットなど、ユーザやディーラーのみが知り得る態様が望ましい）でＩＤ登録モードに切り換わるように変更されてもよい。このようにすれば、モードスイッチ２１を省略することができる。また、モードスイッチ２１の誤操作により、意図しないＩＤ登録モードへの切り換えを防止することができる。なお、車両登録モードに切り換えるための操作を同様に変更してもよい。

【０１０５】

・　前記管理装置３０は、専用の管理センターに限らず、ユーザの自宅などに配設されてもよく、この場合にはパーソナルコンピュータなどによって構成されてもよい。

・　前記実施形態において、携帯電話４は、所定の音声コマンドが音声入力された際に、制限要求信号を管理装置３０に送信するようになっていてもよい。

【０１０６】

また、携帯電話４と管理装置３０との間の通信は、管理装置３０が配設された管理センターに駐在しているオペレータとユーザとの会話によって行われてもよい。すなわち、ユーザは、携帯電話４を用いて管理センターに電話をかけ、オペレータとの会話により、制限要求を指示するようになっていてもよい。この場合、指示を受けたオペレータは、該指示に基づいて管理装置３０を操作し、機能制限制御を行うこととなる。このようにすれば、制限要求信号を、携帯電話４から管理装置３０に送信させる必要がなくなる。

【０１０７】

・　セキュリティ機器は、ドアロック駆動装置２２やエンジン制御部２３に限らず、例えば、ステアリングロック装置、シフトロック装置、タイヤロック装置などであってもよい。つまり、正常な車両２の走行を制限または阻害するための装置であればセキュリティ機器として適用可能である。

【０１０８】

・　セキュリティ制御システムは、車両のセキュリティ機器を制御する車両用セキュリティ制御システム１に限らず、例えば建物用ドアの施解錠を制御する建物用セキュリティシステムとして具体化されてもよい。

【０１０９】

次に、特許請求の範囲に記載された技術的思想のほかに、前述した実施形態によって把握される技術的思想を以下に列挙する。

（１）　請求項１～５のいずれか１項に記載のセキュリティ制御システムにおいて、前記管理装置は、前記携帯機または前記セキュリティ制御装置に前記機能制限信号を送信し

た際には、その旨を示す報知信号を、ユーザによって所持される携帯機機器に送信すること。この技術的思想（１）に記載の発明によれば、ユーザは、機能制限されている旨を確実且つ迅速に認識することができる。

【０１１０】

（２）　請求項１～５、技術的思想（１）のいずれか１項に記載のセキュリティ制御システムにおいて、前記セキュリティ制御装置は、前記セキュリティ通信手段と前記制御手段と間で互いが正常に動作しているか否かの相互認証を行い、該相互認証が成立しない場合には、前記携帯機との通信に基づく前記セキュリティ機器によるセキュリティ解除動作を禁止すること。この技術的思想（２）に記載の発明によれば、例えばセキュリティ通信手段が取り外されたり破壊されたりした場合にはセキュリティ解除動作が禁止されるため、不正なセキュリティ解除動作をより確実に防止することができる。

【０１１１】

（３）　請求項１～５、技術的思想（１），（２）に記載のセキュリティ制御システムにおいて、前記セキュリティ制御装置は車両用であり、前記セキュリティ機器は、ドア錠の施解錠を制御するドアロック駆動装置、エンジンの始動許可を制御するエンジン制御部のうちの少なくとも一方を含んでいること。

【０１１２】

（４）　請求項１１に記載のセキュリティ制御方法において、ユーザによって所持される携帯通信機器を操作することにより、該携帯通信機器から前記管理装置に前記制限要求信号を送信すること。

【図面の簡単な説明】

【０１１３】

【図１】本発明を車両用セキュリティ制御システムに具体化した一実施形態の概略構成を示すブロック図。

【図２】車両登録制御時における通信態様を示すシーケンスチャート。

【図３】ＩＤ登録制御時における通信態様を示すシーケンスチャート。

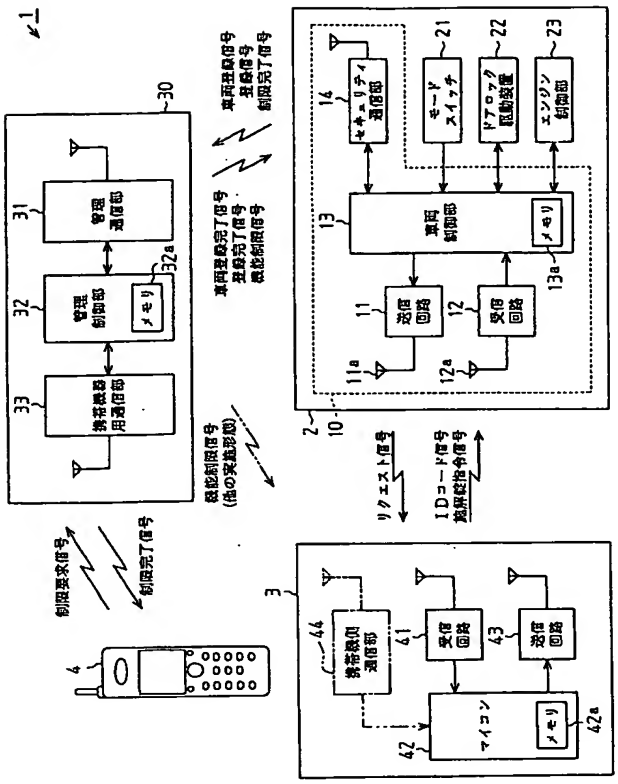
【図４】機能制限制御時における通信態様を示すシーケンスチャート。

【符号の説明】

【０１１４】

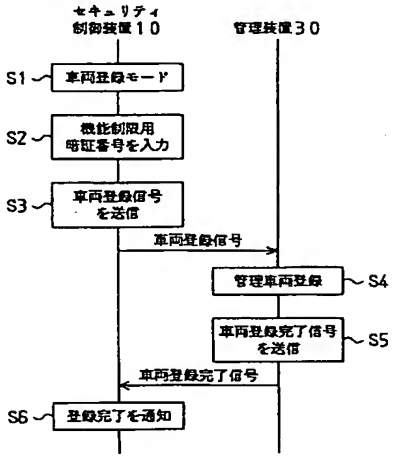
１…車両用セキュリティ制御システム、２…車両、３…携帯機、４…携帯通信機器としての携帯電話、１０…セキュリティ制御装置、１３…制御手段としての車両制御部、１３ａ…記録手段としてのメモリ、１４…セキュリティ通信手段としてのセキュリティ通信部、２２…セキュリティ機器としてのドアロック駆動装置、２３…セキュリティ機器としてのエンジン制御部、３０…管理装置、３１…管理通信部、３２…制限制御手段としての管理制御部、３３…携帯機器用通信手段及び受信手段としての携帯機器用通信部。

【図１】



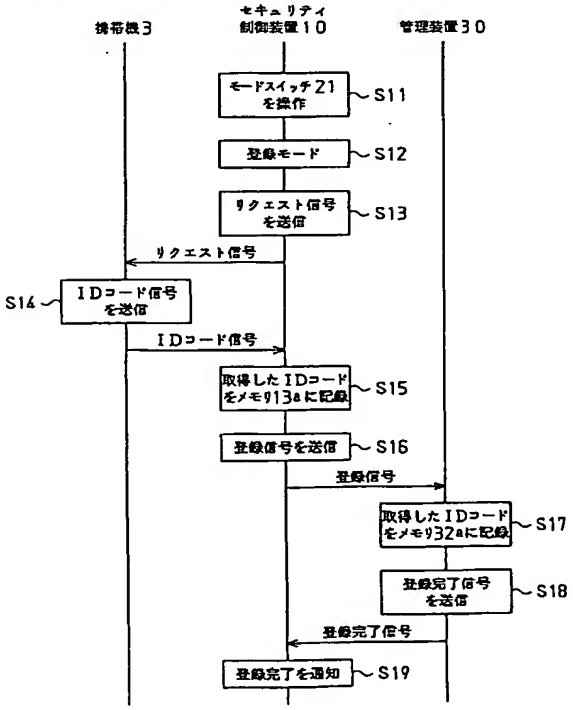
【図２】

(車両登録制御時における通信態様)



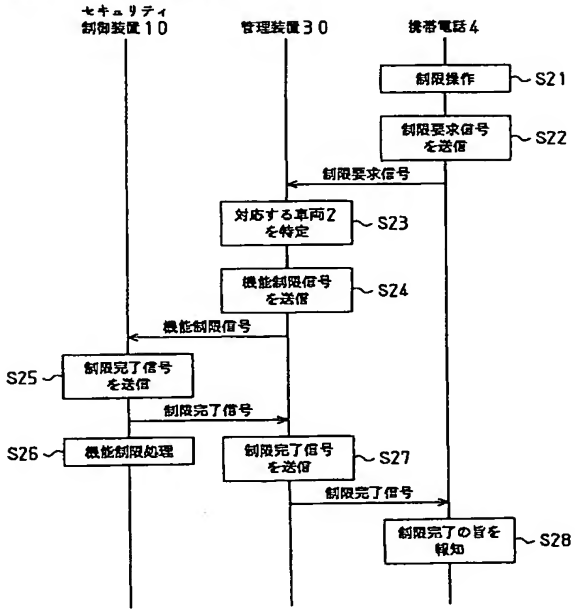
【図３】

(ＩＤ登録制御時における通信態様)



【図４】

(機能制限制御時における通信態様)



フロントページの続き

(72)発明者 木村 明人
愛知県丹羽郡大口町豊田三丁目２６０番地 株式会社東海理化電機製作所内
(72)発明者 山本 圭司
愛知県豊田市トヨタ町１番地 トヨタ自動車 株式会社内
(72)発明者 正村 浩一
愛知県豊田市トヨタ町１番地 トヨタ自動車 株式会社内
(72)発明者 小沢 隆夫
愛知県豊田市トヨタ町１番地 トヨタ自動車 株式会社内
(72)発明者 中根 吉英
愛知県豊田市トヨタ町１番地 トヨタ自動車 株式会社内

Ｆターム(参考) 2E250 AA02 AA03 AA12 AA21 BB08 BB29 BB35 BB36 BB48 BB59
BB61 BB66 CC16 CC19 CC25 DD01 DD06 EE06 FF22 FF23
FF24 FF25 FF27 FF36 GG04 GG07 GG08 GG13 GG15 HH02
JJ03 JJ05 KK03 LL00 LL01 LL18 RR00 SS01 SS03 SS04
SS08 SS09 TT03 UU01 VV00
5K011 JA01 LA08
5K067 AA21 BB04 DD11 DD17 DD27 EE02 EE12 EE35 FF02 FF07
HH22 HH23